LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

BRING YOUR OWN DEVICE

Lamk student -verkon parannussuunnitelma

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2015
Juuso Heromaa

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

HEROMAA, JUUSO:

Bring your own device
Lamk student -verkon
parannussuunnitelma

Tietoliikennetekniikan opinnäytetyö, 39 sivua, 3 liitesivua

Kevät 2015

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli arvioida Muotoilu- ja Taideinstituutin Lamk student -verkon nykyinen tilanne, suorittaa langattomalle verkolle reaaliaikaiset mittaukset ja tehdä parannussuunnitelma näiden mittauksien pohjalta. Lahden ammattikorkeakoulun Tietohallinnon on määrä tehdä parannukset langattomaan verkkoon tämän opinnäytetyön tulosten perusteella.

Lähiverkko tarkoittaa langallista yhteyttä työasemien tai verkkolaitteiden välillä. Langallisen yhteyden kautta verkossa toimivat laitteet pystyvät kommunikoimaan keskenään ja etenkin yritykset käyttävät verkkoyhteyttä tiedon lähettämiseen ja vastaanottamiseen.

Langaton lähiverkko kattaa lähes kaikki samat piirteet kuin langallinen lähiverkkokin, mutta tiedonsiirto tapahtuu ilmateitse radioaaltoja hyödyntäen. Liikkuvuus ja yhteyden luominen lähes mistä tahansa ovatkin langattomuuden vahvuuksia verrattuna langalliseen yhteyteen. Langaton yhteys vaatii kuitenkin tarkemman katselman turvallisuuteen, joka suoritetaan salausalgoritmeilla.

Muotoilu- ja Taideinstituuttiin suoritettavat langattoman verkon mittaukset toteutettiin erillisellä ohjelmalla, jolla pystyttiin määrittelemään tukiasemien sijainteja, kuuluvuusalueet desibeleinä ja tukiasemien kanavien hallintaa. Instituutin pohjapiirrustuksiin luodut kuuluvuuskartat analysoitiin ja näiden kuuluvuuskarttojen perusteella luotiin parannussuunnitelma Lamk student -verkolle.

Parannussuunnitelma pohjaitui mitattujen kuuluvuuskarttojen ja nopeustestien analysointiin. Suunnitelmassa keskityttiin tukiasemien sijaintien optimoimiseen siten, että kuuluvuusalue peittäisi katvealueet ja parantaisi kapasiteettia opetustiloissa. Suunnitelmassa otettiin myös kantaa langattoman verkon parantamiseksi tulevaisuuden kannalta, jossa ehdotettiin langattoman verkon pidemmän ajan mittaukset ja testiympäristön luominen kapasiteetin sekä kuuluvuusalueen merkittävämpään parantumiseen.

Asiasanat: WLAN, langaton lähiverkko, Ethernet, verkkosuunnitelma

Lahti University of Applied Sciences
Degree Programme in Information Technology

HEROMAA, JUUSO:

Bring your own device
Improvement plan for the Lamk student wireless network

Bachelor's Thesis in telecommunications, 39 pages, 3 pages of appendices

Spring 2015

ABSTRACT

The goal of this thesis was to evaluate the current state of the Lamk student wireless network of the Institute of Design and Fine Arts, perform real-time measurements and make an improvement plan based on these measurements. The IT management of Lahti University of Applied Sciences is supposed to execute improvements for the Lamk student network based on the results of this thesis.

A local area network is a cable connection between workspaces and network devices. Cabled connection allows devices operating in the network to communicate and especially corporations use these networks to exchange data.

A wireless local area network includes all the same qualities as a LAN, but communication occurs via air using radio waves. Mobility and the possibility to establish connection to the wireless network from almost everywhere are the strengths compared to a normal LAN. Wireless connection is easy, but it requires great security properties, which are accomplished with encryption algorithms.

Measurements performed on the WLAN of the Institute of Design and Fine Art were done with specialized software, which allows specifying for access point locations, channel management and coverage area as decibels. Coverage areas created on the Institute's layouts were analyzed and improvement plans were done based on these analyses.

The improvement plan is based on the measured coverage area and speed tests. The plan is focused on optimizing access point locations so that the coverage area and network capacity would improve on blind spots. The plan also considers future improvements for the Lamk student network, such as long-term wireless network measurements and creating a testing environment for a greater upgrade of the wireless network.

Key words: WLAN, wireless local area network, Ethernet, planning of network

SISÄLLYS

LYHENNELUETTELO

802.11i	Langattomien 802.11-verkkojen viimeisin tietoturvastandardi.
AES	Advanced Encryption Standard, tietoliikenteessä käytettävä lohkosalausmenetelmä.
Bitti	Tietotekniikassa tiedon tai tietovuon pienin käsiteltävä osa.
CCMP	Counter Mode with CBC-MAC Protocol, langattomassa tietoliikenteessä käytettävä salausprotokolla.
Hz	Hertsi, taajuuden yksikkö, joka kuvaa tietotekniikan komponenttien kellotaajuutta.
IEEE 802	IEEE-standardointijärjestön työryhmä 802, standardoi verkkotekniikkaa.
LAN	(Local Area Network) kaapeloitu lähiverkko, jossa verkkolaitteet liikennöivät keskenään.
PNG	Portable Network Graphics, häviötön bittikarttagrafiikan tallennusformaatti.
RADIUS	Remote Authentication Dial In User Services, sisäänsoittipalveluissa tapahtuvaan tunnistautumiseen käytettävä protokolla.
WAP	Wireless Access Point. Liityntäpiste, joka mahdollistaa langattomien laitteiden liittymisen langalliseen kiinteään verkkoon.

1 JOHDANTO

Lahden ammattikorkeakoulu (LAMK) ottaa käyttöön syyslukukaudella 2015 BYOD (Bring Your Own Device) -nimisen projektin, jonka tarkoituksena on monipuolistaa opiskelijoiden opiskelua heidän omilla laitteillaan. LAMK:lle on aikaisemmin jo luotu oma langaton lähiverkko (WLAN), Lamk student, joka on suojattu, mutta opiskelijoille jaetaan Service Set Identifier (SSID) -tunnus, jolla he pääsevät liittymään verkkoon. Lamk student -verkon on tarkoitus toimia vain ainoastaan LAMK:n tiloissa ja tukea opiskelijoita heidän opinnoissaan. Tietohallinto on pyytänyt, että Lamk student -verkon kattavuus kartoitettaisiin Ståhlberginkadun Tekniikan alan ja Kannaksenkadun Muotoilu- ja Taideinstituutin tiloista. Tämä opinnäytetyö käsittelee Muotoilu- ja Taideinsituutin verkkoa, ja työssä esitellään mitatut tulokset pohjapiirustuksineen. Opinnäytetyö myös perehdyttää lukijan langattoman lähiverkon perusteisiin, ominaisuuksiin, sovellettavuuteen ja turvallisuuteen.

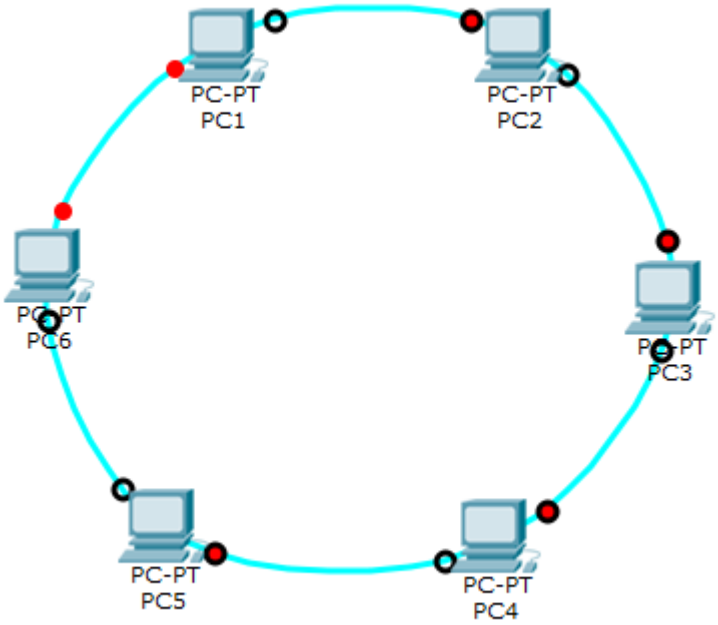
Muotoilu- ja Taideinsituutin tiloissa Lamk student -verkon osalta ongelmana on ollut verkon huono kuuluvuus ja käyttäjien yhteyskatkokset. Tässä työssä käsitellään Lamk student -verkon tilannetta graafisten kuuluvuuskarttojen avulla, jotka on mitattu reaaliajassa Ekahau Site Survey -ohjelmistolla. Ekahau-ohjelma mahdollistaa verkon mittaamisen, suunnittelun ja analysoinnin. Normaalien verkkosuunnitelma käytäntöjen mukaan tässä työssä ei esitellä mallia, jossa on tehty ensin verkon kartoittaminen ja sen jälkeen toteutettu testiympäristö vastaamaan nykyistä tilannetta sekä suorittaa pitkäjänteistä verkontestausta, jonka pohjalta tehdään parannussuunnitelmat. Tässä työssä on käytetty avuksi Ekahau:n Auto-Planner-ominaisuutta, jolla pystyy suunnittelemaan verkon parannukset graafisiin kuuluvuuskarttoihin.

2 LÄHIVERKOSTA YLEISESTI

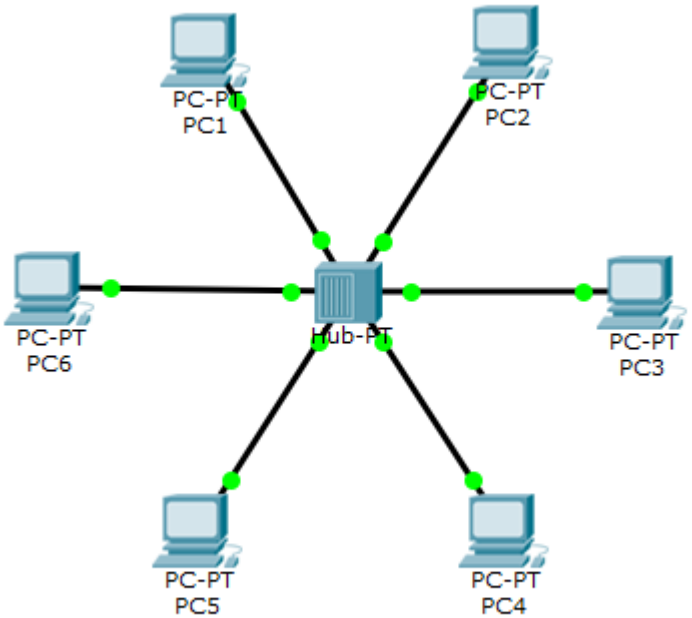
Lähiverkko (Local Area Network, LAN) tarkoittaa langallista yhteyttä laitteiden, kuten työasema tai järjestelmälaite, välillä. Lyhyesti kuvailtuna lähiverkko tarkoittaa yritykselle tai yksityiselle henkilölle rakennettua verkostoa, jossa laitteet pystyvät kommunikoimaan ja jakamaan tietoja. Lähiverkko sai ensimmäisen kerran muotoa Cambridgen yliopistossa vuonna 1970, mutta varsinaisesti tekniikka ja toimiva ympäristö kehitettiin vasta 1973-1975 välisenä aikana Yhdysvalloissa PARC (Palo Alto Research Center Incorporated) -nimisen yrityksen toimesta (Wikipedia 2015b; Wikipedia 2015d.) Toimiva lähiverkko ei varsinaisesti vaadi yhteyttä ulkoverkkoon (Internet), mutta mahdollisuudet ja käytettävyys paranevat ulkoverkkoon liittämisen myötä. Laitteet voivat tarvita päivityksiä, jotka voi ladata vain laitevalmistajan sivuilta ja tällöin lähiverkon liittäminen ulkoverkkoon on tärkeää, mutta tietoturvallisuuden kannalta välttämättömät ohjelmat, kuten palomuuri, täytyy olla ajantasalla ja käyttäjien koulutustaso riittävän korkea. Yleisimmin lähiverkko liitetään ulkoverkkoon kuitiyhteydellä (Ethernet), mutta lähes yhtä yleinen on suurimmassa osassa kotitalouksissa käytettävä kaapeliyhteys. Molemmat edellä mainituista yhteysmuodoista tulevat suoraan palvelun tarjoajalta. (Wikipedia 2015c)

Kaikki lähiverkkotekniikka kuuluu IEEE 802 (Institute of Electrical And Electronics Engineers) -perheeseen, jossa kehitetään ja julkaistaan tiedonsiirtoon liittyviä standardeja. IEEE 802 -perhe on järjestetty sitä varten, että verkossa liikkuessa olisi tietyt säännöt, muutoin virhemarginaali datan, eli tiedon, häviämiselle tai korruptoitumiselle olisi hyvin suuri. Data kulkee lähiverkossa paketteina, joissa on kaikki tarvittava tieto sisällä määränpäästä ja siitä mistä paketti tulee sekä mitä se tietenkin pitää sisällään (EE Herald 2015). Verkossa laitteet tunnistava toisensa MAC-osoitteen (Media Access Control) kautta, joka on jokaiselle laitteelle verkkosovittimen yksilöity osoite. Ethernet on standardi-perheestä käytetyin, mutta ei ainut. Muita tekniikoita ovat esimerkiksi Token Ring (KUVIO 1), jossa ympyränmuotoisessa topologiassa järjestelmälaitteet saavat kommunikoida vain valtuuden (Token) kierrättämisellä. Ethernetissä taas puolestaan käytetään tähdenmuotoista topologiaa (KUVIO 2), jossa tieto välittyy järjestelmälaitteille tai työasemille verkonhallinta laitteiden (reititin, kytkin)

kautta. Lähiverkon koko taas määrittelee, kuinka monta verkonhallintalaitetta tarvitaan. (Axis 2015)



KUVIO 1. Token Ring



KUVIO 2. Ethernetin tähtitopologia

Lähiverkossa tiedonsiirron kannalta tärkeä osa on CSMA/CD (Carrier-Sense Multiple Access with Collision Detection) -varausmenetelmä, joka estää datapakettien törmäämisen verkossa. CSMA/CD on vähän kuin sujuvasti toimiva autotie, verkossa olevat laitteet kuuntelevat ethernet-segmenttiä liikenteen varalta. Käytännössä tämä tarkoittaa kaapelin jännitetason mittaamista, mutta kuunteleminen on parempi termi. Mikäli laite kuulee toisen laitteen lähettävän liikennettä verkkoon, odottaa laite lähetyksen loppuun ja tarkistaa kaistan tilanteen. Jos kaista on tyhjä, laite voi aloittaa oman lähettämisensä. Langattomassa lähiverkossa (WLAN) käytetään samankaltaista varausmenetelmää (CSMA/Collision Avoidance), mutta se perustuu törmäyksien estämiseen siirtotiellä, jota käyttää useat laitteet yhden aikaisesti. Käytännössä tämä tarkoittaa sitä, että laite lähettää siirtotietä varaavan signaalin ennen varsinaista dataa. Mikäli molemmissa menetelmissä tapahtuu datan törmäys, lisääntyy seuraavalle lähetykselle satunnaisesti aikaa, milloin data lähetetään. Mikäli törmäys tapahtuu uudelleen, lisätään jälleen samaista aikaa datan lähetykseen. Satunnaisajan lisäämistä tapahtuu niin kauan, kunnes törmäily loppuu; usein kuitenkaan törmäykset eivät ole suuri haitta ja satunnaisaikaa ei tarvitse lisätä kuin kerran. (Webopedia 2015a)

3 LANGATON LÄHIVERKKO

Lähiverkossa tiedonsiirtoon käytettävät kaapelit ovat kehittyneet koaksaalikaapeliin asti, joka on kevyempää ja helpommin asennettavissa olevaa kuin edeltäjänsä. Lähiverkon rinnalle oli kuitenkin tarve saada kaapelia, joka on yksinkertaisempaa ja edullisempaa; kaapeloinnissa on kuitenkin suhteellisen paljon asennustyötä kaapelin koosta riippumatta (Lowe 2013, 148). Norman Abramson kehitti jo vuonna 1971 ensimmäisen WLANin seitsemän tietokoneen kesken Havaijin saarten välille. WLANiin käytettävä tekniikka kuitenkin tuona aikana oli kallista ja sitä käytettiin vain vaihtoehtoisena ratkaisuna lähiverkolle, jossa kaapelointi oli hankalaa tai jopa mahdotonta (Wikipedia 2015h).

1990-luvun lopulla WLANin protokolla ja laitevalmistajien tekniset ratkaisut korvattiin IEEE 802.11 -standardeilla, ja tästä lähti langattoman lähiverkkotekniikan kehitys sellaiseksi kuin se on nyt (IEEE 802.11n standardi). IEEE 802.11n -standardin suurimpia edistyksiä edeltäjiinsä verrattuna on kahdella taajuudella, 2,4 GHz (Gigahetrsi) ja 5,0 GHz, toiminen saavuttaen maksimi tiedonsiirtokapasiteetin 600 Mbit/s (Megabittiä per sekunti). Nykyaikaisimmat langattomat reitittimet osaavat hyödyntää molempia tajuusalueita mahdollistaen taajuuden vaihdon. Bluetooth-laitteet, mikroaaltouunit sekä radio-ohjattavat lennokit käyttävät 2,4 GHz:n taajuutta, joten langaton reititin ei ruuhkaudu muista laitteista jos se on säädetty taajuudelle 5,0 GHz. (Wikipedia 2015h; Verkkokauppa.com 2015)

3.1 Radiosignaali

WLANissa radiosignaali kulkee sähkömagneettisena aaltona lähettimestä vastaanottimeen antennien välillä. Radiosignaaleja ei luonnollisesti pysty havaitsemaan ihmissilmällä, mutta vastaanottava laite pystyy muuntamaan radiosignaalin ääneksi, kuviksi tai dataksi. Itse radiosignaali koostuu kolmesta elementistä: taajuudesta, vaiheesta ja amplitudista. Radiosignaalit ovat aaltomaisia sähköpulsseja, jotka toistuvat tietyllä aikavälillä, eli taajuudella. Kun puhutaan taajuuksista, käytetään yleensä käsitettä Hertsi (Hz) tai yksikköä 1/s (1 Hz = 1/s). Yksikkö 1/s kertoo, kuinka monta kertaa tapahtuma toistuu sekunnin sisällä: 300

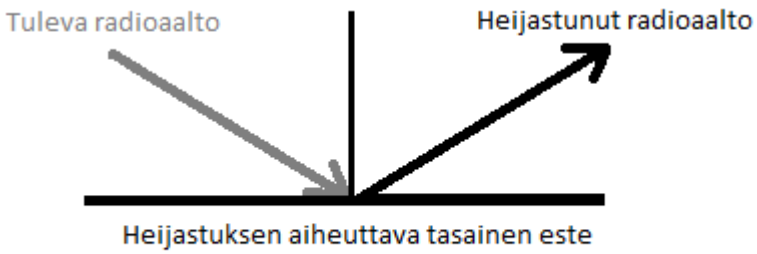
Hz:n taajuudella radiosignaali toistuu 300 kertaa sekunnissa (Lowe 2013, 149, Suomen Standardoimisliitto 2002, 11). Vaiheella tarkoitetaan radioaallon sen hetkistä liikettä, ja lähettimen ja vastaanottimen välinen matka määrittelee radioaallolle vaiheen. Vaiheeseen liittyy myös vaihe-ero, joka tarkoittaa kahden aallon eroa, kuinka paljon heijastusta ottanut aalto tulee suoraa aaltoa jäljessä (Wikipedia 2015e). Amplitudi on signaalin voimakkuus, joka heikkenee mitä pidemmälle signaali kantautuu. Langattomissa verkoissa etäisyydet eivät ole juurikaan suuria ja tukiasemia pyritään sijoittamaan siten, että heikkenemistä ei pääse tapahtumaan suuria määriä nimenomaan kantaman vuoksi. Palveluntarjoajalle amplitudi tuottaa erityisesti haittaa haja-asutusalueilla (Wikipedia 2015a).

Langattomuus ei kuitenkaan ole itsestäänselvyys ja langattomuus sisältää monta haittatekijää. Pelkästään jo tietoturvan kannalta langattomuus tuo paljon haasteita lähiverkkoympäristöön: Verkkoon murtautuminen ja sitä kautta tietojen urkinta, varastaminen sekä jopa sabotointi ovat varteenotettavia uhkia tämänpäiväisessä maailmassa, jossa elämme. Mikään näistä uhkista ei tietenkään ole uusi asia, samat pätevät yhtä lailla tavalliseen kaapeloituun lähiverkkoon, mutta eittämättä langattomuus tuo mukanaan etäämmän ja huomaamattomamman pääsyn verkkoon. Langattomuuden mukana tulee myös lukuisia muita ominaisuuksia, jotka eivät suoranaisesti ole uhkia, mutta joista voi aiheutuu häiriötä:

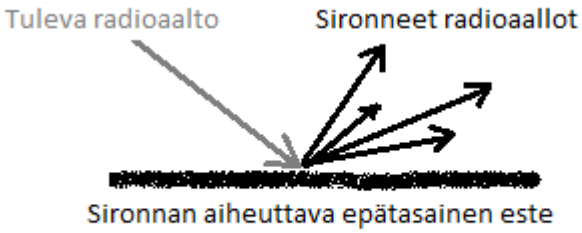
- heijastuminen
- sironta
- taipuminen
- häipyminen.

Heijastuminen tarkoittaa radioaallon osumista tasaiseen esteeseen, josta radioaalto heijastuu samassa kulmassa (heijastuskulma) pois, kuin tulokulma. Radioaalto kuitenkin säilyttää aallonpituuden ja etenemisnopeutensa heijastuksesta riippumatta (KUVIO 3). Sironnan aiheuttaa puolestaan epätasainen este tai pinta, johon radioaalto osuu. Esteen epätasaisuuden täytyy kuitenkin olla pienempi tai yhtä suuri kuin aallonpituus, jotta sirontaa tapahtuu. Sironnasta syntyy uusia radioaaltoja eri suuntiin ja yleisesti heikentää signaalia (KUVIO 4). Taipuminen

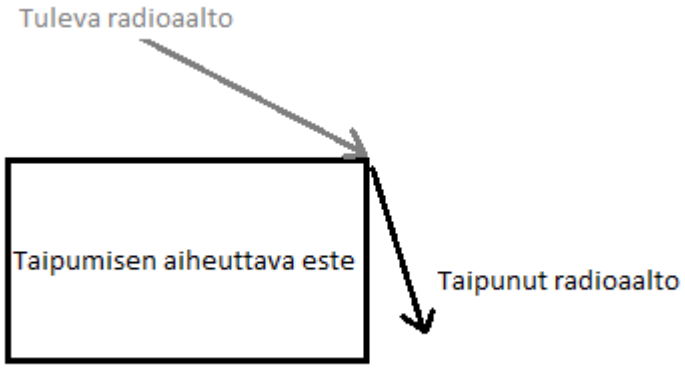
taas puolestaan tapahtuu esteistä, jotka ovat huonosti läpäistävissä tai tasaisia ja radioaalto osuu kulmakohtaan. Taipumisella ei ole yleisesti ole heikentävää vaikutusta signaaliin (KUVIO 5). Hyvin yleinen, etenkin käyttäjien liikkuessa, tapahtuva ominaisuus radioaallolle on häipyminen. Häpymisen aiheuttaa lähettävän tai vastaanottavan laitteen liike, laite ikään kuin karkaa poispäin tai tulee liian nopeasti kohti. (Juutilainen 2007)



KUVIO 3. Heijastuminen ei vaikuta signaalin vahvuuteen ja heijastunut radioaalto säilyttää kulman



KUVIO 4. Radioaallon sironta



KUVIO 5. Radioaallon taipuminen

3.2 Paketit ja kehykset

Tiedonsiirrossa data kulkee paketteina LANissa ja WLANissa ja pitää sisällään kaikki tiedot saapumispaikasta määränpäähän, ja tietenkin itse datan. Paketit kulkevat OSI-mallissa (otsikko 3.6) pääsääntöisesti fyysisessä kerroksessa, mutta siirtoyhteyskerros kehystää paketin fyysisen kerroksen tiedonsiirtoa varten. Paketin sisällä tieto on siis kehystetty eri osioihin, joilla on aikaisemmin mainitusti tärkeä rooli tiedon kulkeutuessa oikeaan osoitteeseen. Datan kehystämiselle on erilaisia tapoja, mutta kaksi niistä on vakiintunut ja yleisimmin käytettyjä nykyajan tiedonsiirrossa:

- Ethernet II
- IEEE 802.3.

Ethernet II (KUVIO 6) on näistä kahdesta käytetympi, koska se on yksinkertaisesti selkeämpi. IEEE 802.3 (KUVIO 7) on IEEE 802-instituutin oma kehitelmä Ethernet-kehykselle hieman laajennetummassa mittakaavassa ja sisällöltään myös monimutkaisempi. Periaattessa nämä kaksi Ethernetin kehystyyppiä ovat samanlaisia muutamalla pienellä erolla, mutta verkossa toimivat laitteet tunnistavat molemmat tyypit ja osaavat käyttää niitä samanaikaisesti. (Dummies 2015)

Ethernet II sisältää kuusi osaa:

- tahdistus (Preamble), 8 tavua
- kohdeosoite (Destination address), 6 tavua
- lähdeosoite (Source address), 6 tavua
- tyyppi (Type), 2 tavua
- data, 46 - 1500 tavua
- kehyksen tarkistustiedot (Frame check sequence), 4 tavua.

Kuten mainittu aikaisemmin, IEEE 802.3 on samankaltainen muutamalla pienellä erolla:

- preamble, 8 tavua
- destination address, 6 tavua
- source address, 6 tavua
- pituus (Length), 2 tavua
- DSAP (Destination service access point), 1 tavu
- SSAP (Source SAP), 1 tavu
- CTRL (Control), 1 tavu
- data, 46 - 1500 tavua
- FCS, 4 tavua.

Preamble-kehys muodostuu vaihtelevista binäärinumeroista nolla (0) ja yksi (1) ja loppuu kahteen 1:een. Tämä kehyksen aloittava numerosarja on käytännössä purskeita, jotka verkkolaitteen verkkokortti havaitsee. Preamblen on tarkoitus tahdistaa vastaanottava laite lähettävän laitteen kanssa samalle kellotaajuudelle. Destination ja source address sekä type voidaan laskea yhdeksi kappaleeksi kehyksessä ja sitä nimitetään yleensä ylätunnisteena (header). Destination address sisältää vastaanottavan laitteen MAC-osoitteen, source address vastaavasti sisältää lähettävän laitteen MAC-osoitteen. Type näyttää ylemmän tason protokollaa, joka yleensä on IP-osoite. Data-kehys sisältää nimensä mukaan tietoa, mutta jos kehys sisältää alle 46 tavua dataa, sisällytetään kehykseen täyte-dataa 64:ään tavuun asti. Data- ja preamble-kehyksien välillä pitää aina olla vähintään 64 tavua dataa. FCS-kehystä luotaessa, paketti pilkotaan osioihin ja paketin sisällöstä luodaan kokonaiskuva. FCS-kehyksen tarkoitus on kertoa vastaanottavalle laitteelle

yhteenveto paketista. Paketin saapuessa vastaanottavalle laitteelle laite luo oman FCS-kehyksen ja vertaa sitä lähetettyyn. Mikäli kehykset eivät täsmää, voidaan olettaa, että paketin sisältö on korruptoitunut matkalla kohteeseensa ja paketti hylätään. FCS-kehyksestä käytetään usein myös käsitettä Cyclic Redundancy Check (CRC), mutta nämä kaksi termiä tarkoittavat samaa. (The Dummies 2015)

IEEE 802.3 -kehyksen sisällä olevat DSAP, SSAP ja CTRL ovat osa LLC:n (Logical Link Control) luomaa hallintotietoa. LLC on siirtoyhteyskerroksen ylätunnus ja esittelee tietoja verkkotasolle (3. taso OSI-mallissa). DSAP on kehys, joka kertoo loogiset osoitteet verkkotasolta sille taholle, joka vastaanottaa paketin. SSAP on vastaavasti kehys, joka kertoo verkkotason loogisen osoitteen paketin luojasta. CTRL-kehys puolestaan kuljettaa mukanaan hallinnointiin liittyviä tietoja.

Kehyksen nimi	Preamble	Destination	Source	Type	Data	FCS
Koko (tavua)	8	6	6	2	46 - 1500	4

KUVIO 6. Ethernet II on käytetyin kehystyyppi

Kehyksen nimi	Preamble	Destination	Source	Length	DSAP	SSAP	CTRL	Data	FCS
Koko (tavua)	8	6	6	2	1	1	1	46 - 1500	4
					LLC				

KUVIO 7. IEEE 802.3 -kehys

3.3 WLAN-standardit

WLAN usein käsitetään samana asiana kuin Wi-Fi (Wireless Fidelity, langaton verkkoyhteys), joka on Wi-Fi Alliencen tavaramerkki eikä ole periaatteessa sama asia kuin WLAN. WLANista kuitenkin käytetään kaupallisessa merkityksessä nimistystä Wi-Fi ja langattomat laitteet usein esitellään Wi-Fi-laitteina (Techopedia 2015). Lähiverkkojen käyttöä varten on kehitetty IEEE 802 -standardit, jotka määrittelevät ominaisuuksia ja rajoja langattomille verkoille. IEEE 802 on jaettu 22:een eri osaan, jotka käsittävät fyysisen ja siirtoyhteystasojen näkökulmia verkostoitumisessa. Yleisimmin tunnistetut standardit ovat 802.3 ja Ethernet, 802.11 Wi-Fi sekä 802.15 Bluetooth, mutta aikaisemmin mainitun mukaan standardit ovat kategorioitu välille 802.1 – 22. (Lowe 2013, 153)

Langattomien IEEE 802.11 -standardien (TAULUKKO 1) kehitys on ehkä merkittävimmin käynyt yhteysnopeuksien kasvuun, esimerkiksi ensimmäinen versio 802.11 mahdollisti yhteysnopeuden maksimissaan 2 Mbit/s (Megabittiä/sekunti) tasolle, mutta jo versio 802.11b mahdollisti 11 Mbit/s siirtonopeuden. Tietenkin nämä ovat ideaalisia arvoja, jotka vaativat esteettömän ja häiritsemättömän ympäristön. WLANin kannalta ehkä yksi suurimmista edistyksistä on ollut 802.11n -standardin julkistaminen, joka mahdollisti dual-band (tupla-kanava) -tekniikan. Tukiaseman pystyy käytännössä säätämään, kummalla kanavataajuudella se toimii (2,4 GHz ja 5 GHz). Etenkin 5 GHz:n kanavataajuus ei pelkästään tuo lisää siirtonopeutta, vaan myös vapaata tilaa kanaville. WLAN-standardeilla on myös mahdollisuus toimia eri kaistalla, esimerkiksi 802.11ac pystyy toimimaan 20, 40, 80 sekä 160 MHz:n kaistalla. Luonnollisesti tiedonsiirtonopeus määräytyy käytetyn kaistan kautta: mitä pienempi kaista, sitä hitaampi on yhteysnopeus. (Webopedia 2015b)

TAULUKKO 1. IEEE 802.11 langattomat standardit

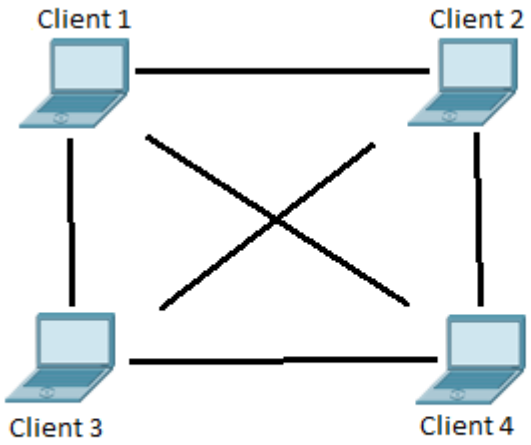
Standardi	Julkaisu vuosi	Taajuus (GHz)	Kaista MHz	Teoreettinen MAX Mbit/s	Modulaatio
802.11	1997	2,4	22	2	DSSS, FHSS
802.11a	1999	5	20	54	OFDM
		3,7			
802.11b	1999	2,4	22	11	DSSS
802.11g	2003	2,4	20	54	OFDM, DSSS
802.11n	2009	2,4 & 5	20	72	OFDM
			40	150	
802.11ac	2013	5	20	96	
			40	200	
			80	433	
			160	866	
802.11ad	2012	60	2160	6900	OFDM

3.4 SSID ja palvelukokonaisuudet

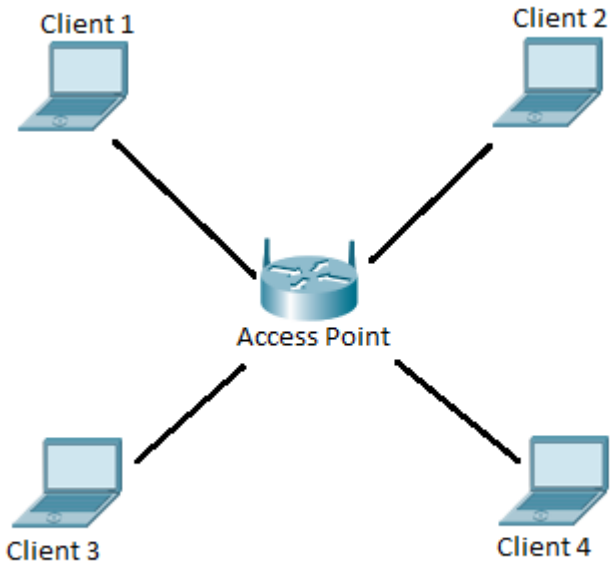
IEEE 802.11 -standardi määrittelee myös langattomassa verkossa käytettävän verkkotunnusta (Service Set Identifier, SSID), jolla pystytään tunnistamaan langattomat verkot toisistaan kun verkkoja on saatavilla enemmän. Datan kulun kannalta SSID -tunnuksen on tärkeää sisältyä verkossa liikkuviin paketteihin, jotta tieto kulkee oikeaan verkkoon. SSID:n pystyy määrittämään selkokieliseksi, ja se voi olla maksimissaan 32 merkkiä pitkä, myös jokaisen langattomaan verkkoon liittyneen laitteen on käytettävä samaa SSID:tä laitteen halutessa liikennöidä muiden verkossa olevien laitteiden kanssa (Techopedia 2015; Wikipedia 2015f). SSID:n lisäksi jokainen laite, liittyessään langattomaan verkkoon, luokitellaan kahteen kategoriaan: liityntäpiste tukiasemiin (Access Point) tai asiakaskäyttäjiin (Client). Erona näillä kahdella kategorialla on se, että AP (Access Point) lähettää ja vastaanottaa radiosignaaleja ja toimii reitittimenä, Client puolestaan luetaan käyttäjäksi, kuten nimikin viittaa, eikä toimi reitittimenä. Toisin sanoen Clientin kautta ei kulje liikennettä, mutta AP mahdollistaa reitityksen avulla datan kulkemisen sen kautta. (Techopedia 2015)

WLANissa useamman laitteen toiminen vaatii standardeja, joiden mukaan edetään. IEEE 802.11 -standardisto on luonut WLAN-verkkoja varten palvelukokonaisuudet (Service Set), jotka määrittyvät täysin aikaisemmin mainittujen AP- ja Client-kategorien mukaan ja langattoman verkon koon. Pienemmässä WLANissa Clientit pystyvät välittämään tietoa toisilleen ilman välikäsiä, ja tätä kutsutaan itsenäiseksi palvelukokonaisuudeksi (Independent Basic Service Set, IBSS) ja mikäli clientit kommunikoivat keskenään erillisen reitittimen kautta hieman suuremmassa WLANissa, kutsutaan tätä silloin peruspalvelukokonaisuudeksi (Basic Service Set, BSS). Kahden saman SSID:n omaavan verkon saaminen ”yhdeksi” langattomaksi verkoksi vaatii laajennetun palvelukokonaisuuden (Extended Service Set, ESS). (Techopedia 2015; Wikipedia 2015f)

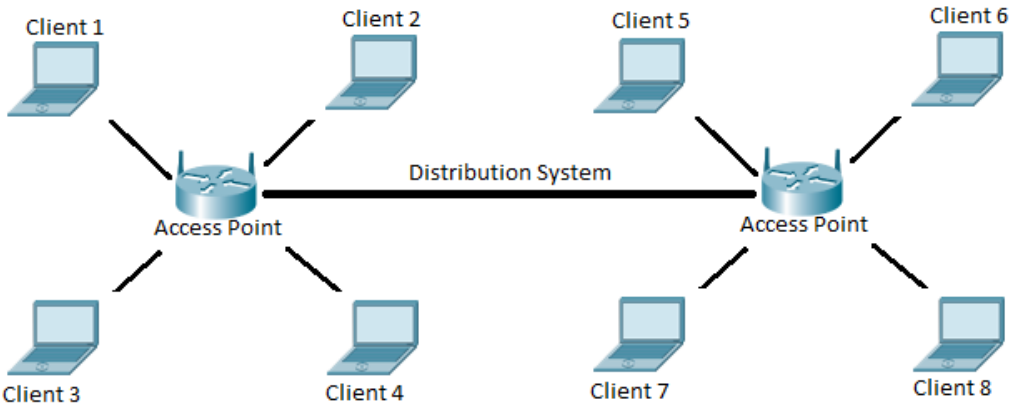
IBSS koostuu langattomista laitteista ja toimii omana pienenä verkkona. IBSS ei mahdollista laitteille pääsyä jakeluverkkoon (Distribution System, DS). IBSS-verkkoa kutsutaan myös nimellä Ad-hoc-verkko (KUVIO 8). Kun itsenäistä palvelukokonaisuutta halutaan laajentaa tai tarvitaan pääsy jakeluverkkoon, tulee ottaa käyttöön AP (tarkennettuna WAP, Wireless Access Point), jonka kautta Clientit liikennöivät. Tällaista verkkoa kutsutaan siis BSS-tukiasema verkoksi, (KUVIO 9) ja se mahdollistaa laajemman käytön langattomassa verkossa. Jokaisella BSS-verkolla on oma BSSID (Basic SSID), jota kaikki tämän kyseisen kokonaisuuden laitteet käyttävät. BSSID on yleensä WAPin 24-bittinen Media Access Control -osoite (MAC). Kahden BSS-verkon yhdistämisessä käytettävä laajennettu palvelukokonaisuus käyttää vain yhtä SSID:tä, vaikka jokaisella BSS-verkolla on oma BSSID. Laajennettu palvelukokonaisuus (KUVIO 10) mahdollistaa pääsyn toiseen peruspalveluverkkoon ja päätelaitteet voivat kommunikoida keskenään jakeluverkon kautta. Tällainen järjestely on erityisen hyödyllinen esimerkiksi liitettäessä kaksi todella lähellä toisiaan olevaa yritysverkkoa kahden WAPin kautta: kaapelointi voi olla vaikeaa tai jopa erittäin kallista sekä työlästä. (Wikipedia 2015f; Lowe 2013, 157 - 158; Techopedia 2015)



KUVIO 8. IBSS on pienimuotoinen Ad-hoc-verkko



KUVIO 9. BSS on isompi palvelukokonaisuus, jossa laitteet liikennöivät Access Pointin kautta



KUVIO 10. ESS on laajempi palvelukokonaisuus, jolla pystytään liittämään kaksi BSS-verkkoa keskenään

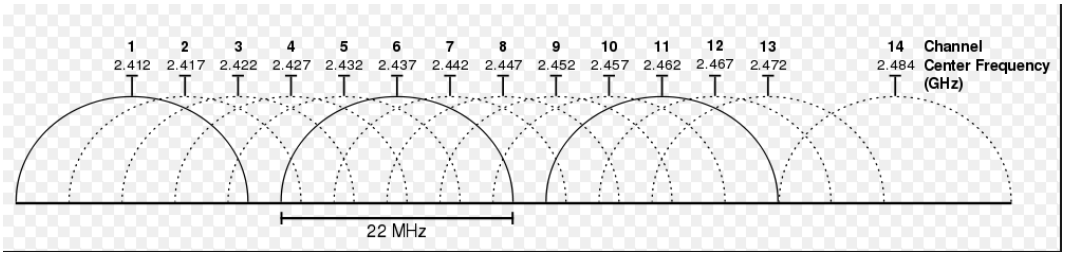
3.5 Kanavat

Langattomassa verkossa liikennöinti tapahtuu kanavia pitkin ja laitteiden pitää olla samalla kanavalla kommunikoidakseen keskenään. Kanavat on myös eritelty taajuuksien mukaan, jotta ylimääräisiltä päällekkäisyyksiltä vältyttäisiin. Täysin päällekkäisyyksiltä ei kuitenkaan pystytä välttymään, ja etenkin jos viereisillä kanavilla on paljon liikennettä, voivat laitteet häiritä toisiaan. Päällekäisyyksiä varten on sovittu, että pääasiassa käytetään tiettyjä kanavia ja pelkästään jo käytettävyyden takia. Päällekäisyydet ovat kuitenkin lähinnä ongelmana enemmän käytetyllä 2,4 GHz:n taajuudella. 5 GHz:n taajuudella on enemmän tilaa laitteille kommunikoida.

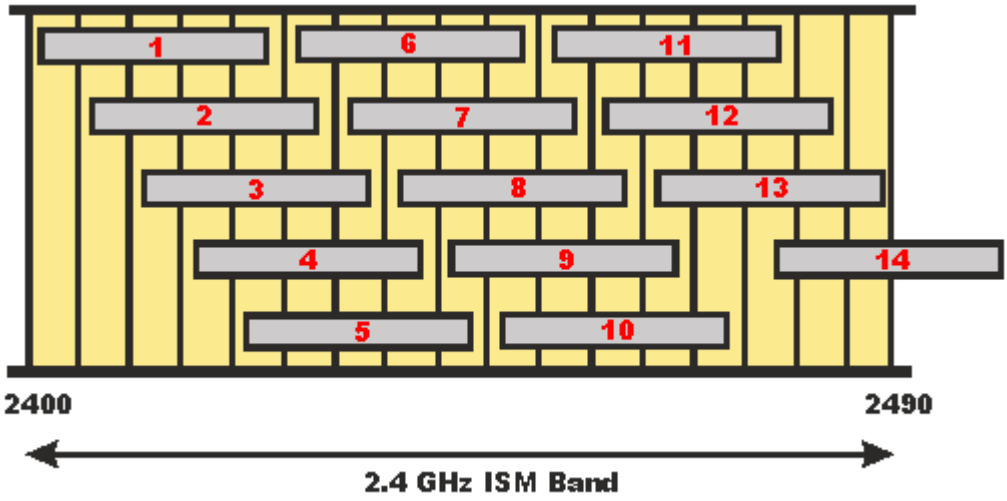
2,4 GHz:n taajuudella kanavat ovat 22 MHz:n kaistoja, mutta kanavien väleille jää vain viiden megahertsin väliset aukot, jotka aiheuttavat päällekäisyyden. Kanavien määrä kuitenkin aihettaa sen, että viisi kolmen kanavan ryhmää eivät mene päällekkäin toistensa kanssa eli ovat erillään (KUVIO 11, KUVIO 12). Kanavien käytön kannalta WLAN-verkon suunnittelussa kannattaakin ottaa huomioon, mitä kanavia on jo käytössä ja voisiko mahdollisesti käyttää jotain

näistä ryhmistä. Yleisesti ottaen käytetään kanavia 1, 6 ja 11, mutta esimerkiksi kanavat 2, 7 ja 12 ovat myös varteenotettava vaihtoehto. Pääpainona kuitenkin täytyy muistaa muidenkin laitteiden liikennöinti ja se, että laitteita ei turhaan häiritsisi. (Radio-electronics 2015)

Kanavien käyttöä on kuitenkin standardien kautta rajoitettu hieman, esimerkiksi Yhdysvalloissa 2,4 GHz taajuuden kanavia saa käyttää vain kanavaan 11 asti, kun taas Japanissa on sallittu käyttää jopa kaikkia 14:ää kanavaa (IEEE 802.11b standardin alla pelkästään). Euroopassa kanavan 14 käyttäminen on kiellettyä (TAULUKKO 2). Myös 5 GHz:n taajuudelle kuuluu rajoituksia ja osa kanavista on varattu pelkästään sisällä käytettäviksi ja osa muihin tarkoituksiin (TAULUKKO 3). 5 GHz:n taajuus alkaa olemaan jo teholtaan niin voimakas, että 5 GHz:n taajuudella toimintaa on ollut pakko rajoittaa. (Extremetech 2014; Radio-electronics 2015)



KUVIO 11. 2,4 GHz taajuuden kanavat (Extremetech 2014)



KUVIO 12. 2,4 GHz:n taajuuden kanavien päällekäisyys kaistoissa (Radio-electronics 2015)

TAULUKKO 2. 2,4 GHz:n kanavien käyttörajoituksia (Extremetech 2014)

CHANNEL NUMBER	EUROPE (ETSI)	NORTH AMERICA (FCC)	JAPAN
1	✓	✓	✓
2	✓	✓	✓
3	✓	✓	✓
4	✓	✓	✓
5	✓	✓	✓
6	✓	✓	✓
7	✓	✓	✓
8	✓	✓	✓
9	✓	✓	✓
10	✓	✓	✓
11	✓	✓	✓
12	✓	No	✓
13	✓	No	✓
14	No	No	802.11b only

TAULUKKO 3. 5 GHz:n kanavien käyttörajoituksia (Extremetech 2014)

CHANNEL NUMBER	FREQUENCY MHZ	EUROPE (ETSI)	NORTH AMERICA (FCC)	JAPAN
36	5180	Indoors	✓	✓
40	5200	Indoors	✓	✓
44	5220	Indoors	✓	✓
48	5240	Indoors	✓	✓
52	5260	Indoors / DFS / TPC	DFS	DFS / TPC
56	5280	Indoors / DFS / TPC	DFS	DFS / TPC
60	5300	Indoors / DFS / TPC	DFS	DFS / TPC
64	5320	Indoors / DFS / TPC	DFS	DFS / TPC
100	5500	DFS / TPC	DFS	DFS / TPC
104	5520	DFS / TPC	DFS	DFS / TPC
108	5540	DFS / TPC	DFS	DFS / TPC
112	5560	DFS / TPC	DFS	DFS / TPC
116	5580	DFS / TPC	DFS	DFS / TPC
120	5600	DFS / TPC	No Access	DFS / TPC
124	5620	DFS / TPC	No Access	DFS / TPC
128	5640	DFS / TPC	No Access	DFS / TPC
132	5660	DFS / TPC	DFS	DFS / TPC
136	5680	DFS / TPC	DFS	DFS / TPC
140	5700	DFS / TPC	DFS	DFS / TPC
149	5745	SRD	✓	No Access
153	5765	SRD	✓	No Access
157	5785	SRD	✓	No Access
161	5805	SRD	✓	No Access
165	5825	SRD	✓	No Access

3.6 OSI-malli

Vuonna 1984 International Organization for Standardizationin (ISO) kehittämä OSI-malli (Open Systems Interconnection) on yksi datan käsittelyn ja ylipäätään verkkoliikenteen kulmakiviä. OSI-malli koostuu seitsemästä eri osasta (KUVIO 13), joilla on oma roolinsa eri tehtävissä, joita verkossa tapahtuu. Perusidea on, että kun jokin tehtävä suoritetaan, se pilkotaan pienempiin tehtäviin ja jaetaan eri OSI-mallin kerrosten kesken. Tehtävän jakaminen pienemmille kerroksille pienentää virhemarginaalia, ja jos kerroksiin täytyy tehdä päivityksiä, ei se häiritse muiden kerrosten toimintaa vaan kohdistuu pelkästään päivitettävään kerrokseen.

OSI-mallin kerrokset on jaettu kahteen isompaan ryhmään: yläkerrokset ja alakerrokset. Yläkerroksen tehtävänä on keskittyä lähes täysin sovelluspohjaisiin

toimintoihin, ja se on lähimpänä loppukäyttäjää, kun taas alakerrokset käsittelevät datasiirtoja koskevia tehtäviä ja ovat lähempänä fyysistä rajapintaa. (Dummies 2015)

	Kerros	Tarkoitus	
7.	Sovelluskerros	Sovellukset	Sovelluskerrokset
6.	Esityskerros	Datan esitysmuoto	
5.	Istuntokerros	Istuntojen hallinta	
4.	Kuljetuskerros	Sovellusten osoittaminen	Kuljetus
3.	Verkkokerros	Verkkojen yhdistäminen	Internet-kerros
2.	Siirtokerros	Vuoronvaraus, linkitys	Verkkoyhteyskerros
1.	Fyysinen kerros	Ethernet	

KUVIO 13. OSI-mallin kaikki kerrokset

3.6.1 Kerrokset

Siirtokerroksen tehtävänä on tarjota sujuvaa tiedonsiirtoa fyysisten verkkoyhteyksien ylitse. Siirtokerroksessa on määritelty erilaisia spesifikaatteja, joka määrittelevät verkko- ja protokolla piirteitä, fyysistä osoitteistusta, verkkotopologiaa, virheenmäärittelyä, datapakettien järjestelyä sekä tiedonkulun hallintaa. Fyysinen osoitteistus määrittelee, kuinka laitteet esitellään siirtokerroksessa, ja verkkotopologia puolestaan määrittelee, miten laitteet tulee fyysisesti kytkeä. Virheenmäärittelyn tehtävä on ilmoittaa datan siirtovirheistä ylemmän kerroksen protokollille, ja datapakettien järjestelyssä puolestaan hallitaan kehyksiä. Viimeisen spesifikaatin, eli tiedonkulun hallinnan, tehtävänä on huolehtia, ettei vastaanottava laite saa liikaa dataa, jota se ei pystyisi käsittelemän. (Dummies 2015; Cisco Press 2015)

Verkkokerroksessa määritellään reititystä ja siihen liittyviä toimintoja, jotka

mahdollistavat siirtotieyhteyksien liittämisen laajempaan verkkokokonaisuuteen. Tämän mahdollistaa laitteiden looginen osoitteistus. Kuljetuskerroksessa puolestaan luodaan tiedonsiirron kannalta kuljetuspalveluita ja tietoja, minne datan tulee päätyä. Istuntokerroksessa nimensä mukaisesti hallitaan, avataan ja suljetaan istuntoja. Istuntojen hallitseminen perustuu palveluiden pyyntö- ja vastausviesteihin verkossa toimivien laitteiden välillä. Esityskerroksessa puolestaan hallitaan, miltä tieto näyttää ja mitä piirteitä sillä on. Esityskerroksen tärkeä tehtävä on myös varmistaa, että omassa sovelluskerroksessa näyttävä data on myös luettavissa olevaa verkossa toimivan toisen laitteen sovelluskerroksessa. Viimeinen kerros, eli sovelluskerros, on lähimpänä loppukäyttäjää, mikä merkitsee sitä, että sovelluskerros ja käyttäjä kummatkin kommunikoivat sovelluksen kautta. (Cisco Press 2015)

3.6.2 Protokolla

OSI-malli ei itsessään ole yksi verkossa kommunkoinnin tavoista vaan tarjoaa raamit päätelaitteiden kommunikointia varten. Itse kommunikointi tapahtuu protokollia käyttämällä. Protokolla käsitteenä tarkoittaa sääntöryhmää ja tapaa, jolla verkossa olevat laitteet kommunikoivat keskenään. Protokolla hyödyntää yhtä tai useampaa OSI-kerroksen käytäntöä, ja kaikki protokollat voidaan jakaa neljään isompaan ryhmään: LAN-protokollat, WAN (Wide Area Network) protokollat, verkkoprotokollat sekä reititysprotokollat. LAN-protokollat toimivat fyysisellä ja siirtoyhteystasolla OSI-mallissa (kerrokset yksi ja kaksi) ja määrittävät liikennöinnin kannalta tärkeitä käytäntöjä. WAN-protokollat toimivat kolmella alimmaisella kerroksella ja määrittävät liikennöinnin käytäntöjä laajemmalle verkkomedialle. Reititysprotokollat ovat verkkokerroksella (neljäs kerros) toimivia käytäntöjä, jotka määrittelevät verkkoreitin hallintaa ja kytkemistä. Viimeisenä ryhmänä on verkkoprotokollat, jotka käsittävät suuren osan yläkerros-ryhmän protokollista. (Cisco Press 2015)

3.7 Tietoturva

Monesti sanotaan jonkin tietyn piirteen olevan tärkeämpi WLANissa kun toisen, mutta todellisuudessa tietoturvallisuus listaantuu prioriteeteissa korkeimpien

joukkoon. Tiedonsiirrolla ja datan säilyttämisellä ei ole mitään perustaa yritykselle jos tietoturva ei ole kunnossa ja dataan on ulkopuolisten mahdollista päästä käsiksi. Nykypäivän tietoverkostossa täytyy olla tarkkana mitä sovelluksia työasemalle asentaa, mistä lähteestä ja millä oikeuksilla. Usein yrityksissä on jaettu henkilöstö oikeuksien mukaan luokkiin, kuka saa tehdä ja mitä. Pääasiassa kaikkeen asentamiseen, muusta kuin omasta yrityksen verkosta, tarvitaan jonkin tasoinen hyväksyntä hyökkäysten tai virusten varalta. Yritykset usein myös haluavat suojata tietojaan hyväksyttämällä tietoturvakäytännöt uudella henkilöstöllä tai henkilöillä, ketkä pääsevät käyttämään yrityksen päätelaitteita. Käytännössä salassapitovelvollisuus on oikeudessa rangaistava teko. Monet laitevalmistajat sekä tietoturvaohjeet suosittelevatkin käyttämään monikerroksista tietoturvamenetelmää, jossa hyökkääjä joutuu niin sanotusti murtautumaan monen eri palomuurin tai salauksen läpi. (Cisco 2015; Tietojenkäsittelytieteen laitos 2015)

3.7.1 Uhkatekijät

Langattomalle verkolle uhkatekijät ovat samoja kuin langalliselle verkolle, joukkoon kuitenkin mahtuu muutamia erilaisia piirteitä, jotka langattomuus mahdollistaa. Vaikka tämän päivän tietoturvamenetelmät ovat laadukkaita, ei se tarkoita etteikö verkkoon pääsisi murtautumaan tai ettei verkko olisi haavoittumaton. Tapoja tunkeutua verkkoon on monia, mutta näistäkin löytyy selkeästi tyypillisimmät tavat. Tyypillisimpiä tietoturvan uhkatekijöitä:

- luvaton laite verkossa
- palvelunestohyökkäykset
- asetusten väärin tai puutteellinen asetus
- verkon kuuntelu ja datan varastaminen.

Luvaton verkkolaite WLANissa toteutetaan usein asettamalla vale-liityntäpiste verkkoon, joka on tunkeutujan kantamalla. Huijauksen idea on yksinkertaisesti hämätä verkossa toimivia laitteita luulemaan, että vale-liityntäpiste tai -laite toimisi kuten muutkin laitteet. Tämäntapainen uhka kuitenkin usein vaatii fyysistä pääsyä verkkoon kaapelilla, jotta valelaite saisi fyysisen osoitteen liikennöidäkseen muiden laitteiden kanssa. Tapa on näiltä osin helposti

estettävissä ja on hyvin heikko uhkatekijä. Huijaus kuitenkin on vaarallinen, jos valeliityntäpiste saa huijattua muita laitteita liittymään tämän jakamaan verkkoon ja liittyneissä verkkolaitteissa ei itsessään ole palomuuriasetukset kunnossa. Mikäli palomuuriasetukset ovat puutteelliset, voi oikeakin verkkolaite luoda tietoturvauhan jakamalla verkkoaan muille laitteille, jotkä pääsevät huonon palomuurin ohitse tekemään vahinkonsa. (Cisco 2015; PlurarSight 2011)

Palvelunestohyökkäykset (DoS, Denial of Service) ovat lisääntyneet huomattavasti viime aikoina sen takia, että DoS on helppo toteuttaa. DoS toimii periaatteltaan siten, että haluttua verkkoa tai palvelua kuormitetaan ylimääräisellä liikenteellä ja pyritään kaatamaan kohteen saatavuus tätä kautta. DoS-hyökkäyksen toteuttaminen vaatii kuitenkin huomattavan määrän liikennettä kohteeseensa, jotta tämä tukkiintuu tai jopa kaatuu, joten välttämättä yhdellä päätelaitteella tätä ei edes pysty suorittamaan. DoS-hyökkäyksen pystyy myös suorittamaan kanavan häirinnällä: 2,4 GHz taajuudella on vain kolme toisistaan erillään olevaa kanavaa, joten hyökkääjän ei tarvitse kuin häiritä joko WLANissa liikkuvia signaaleja tai liityntäpistettä olemalla viereisellä kanavalla tuottamassa paljon liikennettä. Sama periaate toimii myös tapaan, jossa vale-liityntäpiste yrittää aiheuttaa mahdollisimman paljon liikennettä oikean liityntäpisteen viereisellä kanavalla ja sitä kautta saada tämä liityntäpiste hakemaan jatkuvastu uutta kanavaa. Yleensä liityntäpisteiden asetuksissa on määritelty, että laite hakee itse automaattisesti kanavan, joka ei ole ruuhkainen. (PlurarSight 2011)

Vajaavaiset asetukset verkkolaitteissa aiheuttaa myös tietoturvariskin ja tämä on aivan käyttäjäpohjainen virhe. Normaalisti verkkolaitteissa on perusasetukset, joita monikaan, etenkin kotikäytössä, ei muuta tai muokkaa. Huomattavana vaaratekijänä tässä piilee se, että huonosti suojattu verkkolaite voi mahdollistaa hyökkääjälle pääsyn sellaiseen verkkoon, jossa voi olla arkaluontoisia tietoja ja tiedostoja. Verkonkuuntelu taas puolestaan on lähes mahdotonta estää kokonaan pelkästään jo langattoman verkon toimintaperiaatteen puolesta. Kun hyökkääjä pääsee tarpeeksi lähelle, pystyy hän kuuntelemaan verkon liikennettä erilaisilla ohjelmilla ja mahdollisesti löytämään heikkoja kohtia verkossa tai jopa tietoturva-asetuksiin liittyviä arkaluontoisia tietoja. (PlurarSight 2011)

3.7.2 Salaus

Vaikka verkkolaitteessa olisikin muutettu asetuksia, on kuitenkin tärkeää ymmärtää tiedon salaaminen verkkoliikennöinnissä. Salaaminen käytännössä tarkoittaa sitä, että selkokielinen data muutetaan sellaiseen muotoon, jossa siitä ei saa selvää. Periaatteena toimii avain -malli, jossa pelkästään salausavaimen haltijat pystyvät aukaisemaan viestin salauksen. Salaukseen on käytetty monta erilaista standardia aikaisemmin, mutta nykyaikaiset IEEE 802.11 -standardit ovat osa laitteiden perustoimintoja. Salausmenetelmät perustuu algoritmeihin ja näistä merkittävimpiä ovat

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2.

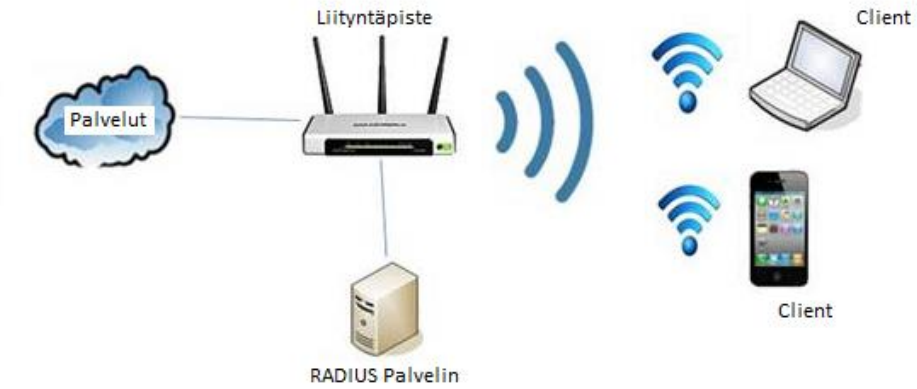
WEP oli ensimmäinen vuonna 1999 esitelty 802.11-standardin salausalgoritmi, joka suojasi työaseman ja tukiaseman välistä liikennettä. Aluksi WEP:n salausavain oli 40 bittiä pitkä, joka oli tarkoituksella rajoitettu Yhdysvaltojen toimesta. Myöhemmin salausavaimen pituuden rajoitus otetiin pois ja salausavaimien pituudet ovat kasvaneet. Käytännössä nykyään salausavaimen pitää olla vähintään 128 bittiä pitkä, jotta salausta ei pysty helposti murtamaan. Periaate salausavaimen takana on yksinkertainen: mitä pidempi salausavain, sitä paremmat mahdollisuudet säilyttää salaus. Vaikka salausavain olisikin pitkä, se ei tarkoita etteikö sitä pystyisi murtamaan siltikin. Pitkän avaimen murtaminen vaatii pitkäjänteistä verkon kuuntelua ja käytännössä tämä tarkoittaa jopa viikkoja. Ottaen huomioon WLANin kantaman, tällainen pitkäjänteinen verkon kuuntelu tulisi ilmi mitä pikemmin. (PlurarSight 2011)

WPA ja WPA2 ovat Wi-Fi Alliancen kehittämiä turvallisuusprotokollia, joista WPA korvasi WEP:n vuonna 2003. Wi-Fi Alliance huomasi, että WEP:ssä on huomattavia heikkouksia ja turvallisuuden kannalta kriittisiä aukkoja, joten oli kehitettävä jotain luotettavampaa. Wi-Fi Alliancen tavoitteena oli luoda salausalgoritmi, joka kattaisi täysin IEEE 802.11i -standardin.WPA oli tarkoitus jakaa verkkolaitteille järjestelmäpäivityksenä ja saada mahdollisimman moni verkkolaite käyttämään WPA-salausta. WPA toi mukanaan uuden

salausmenetelmän TKIP (Temporal Key Intergrity Protocol), joka käyttää salausta jokaisessa datapaketissa. Tämä tarkoittaa käytännössä, että TKIP luo jokaiselle paketille 128-bittisen avaimen, joka on huomattavasti parempi salausmenetelmä, kuin yksi sama avain jatkuvalle liikenteelle. WPA myös mahdollisti viestin eheyden tarkistamisen, joka tarkistaa paketit säännöllisesti kuuntelun, kaappaamisen ja uudelleenlähettämisen varalta. Eheyden tarkistusominaisuus korvasi aiemmin WEP:ssä käytettävän CRC (Cyclic Redundancy Check) -menetelmän, jonka heikkoutena oli liian löyhä pakettien eheyden tarkistaminen. Myöhemmin vuonna 2006 Wi-Fi Alliance julkisti WPA2 salausmenetelmän, joka täytti täysin 802.11i -standardiston. WPA2 toi mukanaan vielä voimakkaammat salausprotokollat CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) sekä AES (Advanced Encryption Standard). (Wikipedia 2015g; PlurarSight 2011)

WPA-salausmenetelmää on myös sovellettu tietyille käyttäjäryhmille: henkilökohtainen WPA-Personal (WPA-PSK) ja lähinnä yrityksille suunnattu WPA-Enterprise (WPA-802.1x, RADIUS), joka vaatii enemmän asetuksia. WPA-PSK-tila on toiminnaltaan yksinkertaisempi näistä kahdesta vaihtoehdosta ja soveltuukin erityisesti koti- tai henkilökohtaiseen käyttöön, kuten nimikin viittaa. WPA-PSK:ssa salasanan asetettua jokaisen liityntäpisteeseen liittyvän käyttäjän täytyy tietää tämä asetettu salasana (KUVIO 14). Suojausasetuksia ei pysty vaihtamaan muuta kautta kuin kytkeytymällä liityntäpisteeseen fyysisesti. Tämä tarkoittaa sitä, että kuka tahansa voisi käytännössä kytkeytyä kiinni liityntäpisteeseen ja kirjautumistunnukset tietäessään mennä vaihtamaan asetuksia. WPA-Enterprise-tilassa autentikointi on henkilökohtaista: RADIUS-palvelimelle on tallennettu käyttäjien 802.1x RADIUS-autentikointi-tiedot ja tätä kautta käyttäjät pääsevät liittymään verkkoon. Tämä tila vaatii kuitenkin huomattavasti enemmän asetuksien määrittämistä ja ylläpitoa, minkä takia sitä suositellaankin suurempien yritysten käyttöön (KUVIO 15). Käyttäjät eivät koskaan pääse tässä tilassa käsiksi luotuun salausavaimeen, vaan salausavain luodaan jokaisella kerralla uusiksi, kun käyttäjä syöttää omat autentikointi -tiedot verkkoon kirjauduttaessa. (TP-Link 2015)

KUVIO 14. WPA-Personal tilassa liittyminen verkkoon (TP-Link 2015)



KUVIO 15. WPA-Enterprise tilassa kirjautuminen isompaan palvelukokonaisuuteen (TP-Link 2015)

3.7.3 Suojautuminen

Suojautuminen hyökkäyksille on tietoturvan avaintekijöitä. Tietopankin kartoitus onkin yksi tärkeimmistä tehtävistä, joka tulisi suorittaa: yritykselle tai henkilölle

tärkeiden tiedostojen kartoitus ja suojata nämä tiedostot sen mukaisesti. Usein kuitenkin vahvin keino estää tietomurto on toteuttaa monikerroksinen suojautuminen palomuureilla ja tunnistautumisilla. Myös käyttäjien oikean mukainen kouluttaminen käyttämään järjestelmää on erittäin tärkeä tapa suojautua. Kun kyse on yrityksen verkosta, täytyy käyttäjillä hyväksyttää salassapitovelvollisuus niiltä osin, ketkä pääsevät luottamuksellisiin tietoihin ja dataan. (Rousku 2013)

Yhtenäinen tietojen luokittelut omiin luottamuskategorioihin on tärkeä vaatimus yritykselle tietojen säilymisen kannalta. Tämä myös koskee tietojen fyysistä varastointia eri tiloihin, jonne on pääsy vain niillä henkilöillä, jotka vastaavat järjestelmästä. Tietoturvauhkien ja hyökkäysten mennessä monimutkaisemmaksi täytyy varmistaa, että kaikista luottamuksellisimpia tietoja käsitellään ympäristössä, josta ei ole pääsyä ulkoverkkoon. Kun järjestelmään tuodaan ulkoverkosta tietoja, täytyy ne tuoda varmojen ja yhdenmukaisten protokollien kautta. Moni yritys onkin kieltänyt omien laitteiden tuomisen yritysverkkoon. Hyökkäyksien kannalta tänä päivänä yksi kiusallisimmista on aikaisemmin mainittu DoS-hyökkäys, jolta myös pystyy suojautua. Suojautumisen idea piilee itse hyökkäyksen ideassa: hyökkäyksessä yritetään lamauttaa järjestelmä suurella määrällä tietoa eli tällöin palvelun kapasiteetti tulee mitoittaa ylisuureksi. Tämä ei kuitenkaan välttämättä ole pienemmille yrityksille kovin edullinen ratkaisu, mutta mikäli yrityksen tietopankki on elintärkeä yritykselle, on syytä miettiä ylimitoitusta. (Rousku 2013)

3.8 Langattoman lähiverkon suunnittelu

3.8.1 Tarpeiden määrittäminen

WLAN-lähiverkon suunnittelussa on tärkeätä kartoittaa, mihin tarkoitukseen ja millaisessa mittakaavassa langaton verkko tulisi olla. Käyttäjien määrä vaikuttaa suoraan kuinka ison kapasiteetin verkko tarvitsee, etenkin paikoissa, joissa on yhdenaikaisesti useaita aktiivisia käyttäjiä. Turvallisuus on myös otettava huomioon yhtenä perusasioista: käytetäänkö WPA-Enterprise- vai WPA-Personal -tilaa. Tilan valintaan vaikuttaa luonnollisesti verkon koko, sillä pienemmässä

verkossa WPA-Personal on taloudellisestikin kannattavampi. Suunnittelussa pitää ottaa huomioon tulevaisuudessa tehtävät uudistukset ja lisäykset: yrityksen kasvaessa suuremmaksi tulee ottaa käyttöön WPA-Enterprise ja suurennettava verkon kapasiteettia. Suunnittelussa kannattaa myös käyttää apunaan palveluita, jotka mittaavat ja kartoittavat verkon yrityksen tarpeisiin: Yksinkertaisilla sovelluksilla pystyy mittaamaan joko nykyisen verkon tilan tai luoda suunnitelma aivan uudesta verkosta. (Signal Partners 2015)

3.8.2 Vaatimukset ja toteutus

Suunnitelman pohjalta tehdään langaton verkko, ja onkin tärkeää katsoa tukiasemille paikat ja niille tarvittavat sähkötyöt. Tukiasemien asetukset ja kanavavalinta on myös olennainen osa toteutusta. Tukiasemat yleisimmin sijoitetaan siten, että ne eivät ole havaittavissa: tämä on jo pelkästään turvallisuustekijä, joka ennaltaehkäisee asiattoman pääsyn tukiasemiin. Tukiasemat voi myös sijoittaa lukittuun tilaan, mutta tällöin pitää huomioida mahdolliset kantavuutta haittaavat tekijät. Tukiasemat tulee siis sijoittaa verkkosuunnitelman mukaisiin paikkoihin ja siten ettei kantavuus kärsi. Huomioon otettavia asioita myös nykyään ovat muut lähellä toimivat langattomat verkot ja se, miten kiinteään verkkoon liittäminen tapahtuu. Suurin osa tukiasemista toimii 2,4 GHz:n taajuudella ja kanavien valinta täytyy tehdä siten, ettei päällekäisyyksiä tule. (Vähä-Touru 2007, 18)

Ennen koko verkon rakentamista on asianmukaista tehdä pienimuotoinen testiympäristö, jossa pystytään tarkentamaan laitteiden asetuksia ja tekemään tarvittavat muutokset. Aikaisemmin mainitut suunnittelutyökalut tarjoavat tähän suuren avun, sillä näillä sovelluksilla pystyy mittaamaan tarkasti halutun verkon kuuluvuuden metrien tarkkuudella. Kanavia asettaessa täytyy huomioida WLANin kuuluvuus kolmiulotteisesti: useassa kerroksessa toimivat tukiasemat voivat häiritä toisiaan, mikäli ne ovat viereisillä kanavilla. Mikäli tukiasemia ja eri verkkoja on monta samassa monikerroksisessa rakennuksessa, täytynee harkita 5,0 GHz:n taajuutta ja tällöin myös sen mukaista laitteistoa. Tällä taajuudella täytyy kuitenkin huomioida 802.11a-standardin huonompi kantavuus verrattuna 2,4 GHz:llä toimiviin standardeihin. Käytännössä tämä tarkoittaa sitä, että mikäli

tavoitteena on toteuttaa suurempi verkko ja taajuutena käytetään 5,0 GHz:ä, niin laitteiden määrä kasvaa lyhyen kantavuuden vuoksi. (Vähä-Touru 2007, 19)

Tänä päivänä langattomiin tukiasemiin on myös mahdollista ottaa käyttöön virtuaalinen lähiverkko (Virtual LAN, VLAN), joka mahdollistaa yhdessä tukiasemassa käytettävän esimerkiksi kahta eri verkkoa. VLANit käyttävät eri SSID-tunnuksia jokaisessa luodussa loogisessa verkossa ja näihin verkkoihin voidaan myös määrittää erilaiset asetukset, esimerkiksi salausasetukset. VLAN vaatii kuitenkin katselmuksen laitteiden ominaisuuksiin: tavalliset tukiasemat eivät tue kuin yhtä SSID:n käyttöä, joten ominaisuuksiltaan laajempien laitteiden hankinta on suositeltavaa. (Vähä-Touru 2007, 19)

4 BRING YOUR OWN DEVICE

4.1 Toimeksianto verkon suunnittelulle

Lahden ammattikorkeakoulu (LAMK) siirtyy syksyn lukukaudella 2015 käyttämään BYOD (Bring Your Own Device) -nimistä menetelmää, jossa ohjataan opiskelijoita tuomaan omia laitteita korkeakouluun tukemaan opiskelujaan. Lahden alueella toimintansa jo pitkälle vienyt MASTOnet on usein käytetty LAMKissa, mutta sen rinnalle on luotu LAMKin oma Lamk student -nimeä kantava opiskelijoille tarkoitettu WLAN. Lamk student -verkon salasana on jaettu vain kyseisen korkeakoulun opiskelijoille ja on tarkoitettu vain opiskelua varten. Lamk student -verkko on kuitenkin suhteellisen alkutekijöissään ja paikoittain Ståhlberginkadun sekä Kannaksenkadun tiloissa käytössä olevassa WLAN-verkossa on puutteellisia peitekohtia. Tämä opinnäytetyö käsittelee Kannaksenkatu 22:ssa sijaitsevan Lahden Muotoilu- ja taideinstituutin tiloja sekä sen Lamk student -verkkoa.

Ammattikorkeakoulun tietohallinnon pyynnöstä on aloitettu mittaukset Lamk student -verkon toimivuudesta ja mahdollinen parannussuunnitelma. Tekniikan laitoksen tiloissa pidetyssä kokouksessa nousi esille muun muassa

- Lamk student -verkon nykyinen tila
- Muotoilu- ja Taideinstituutin WLANin ulottuminen ulkotiloihin
- verkon mahdolliset ongelmakohdat ja käyttäjien putoaminen verkosta
- mittauksien ulottuminen vain niihin tiloihin, joihin opiskelijoilla on pääsy
- verkon kapasiteetin testaus, mikäli mahdollista.

4.2 WLAN-verkon mittaukset

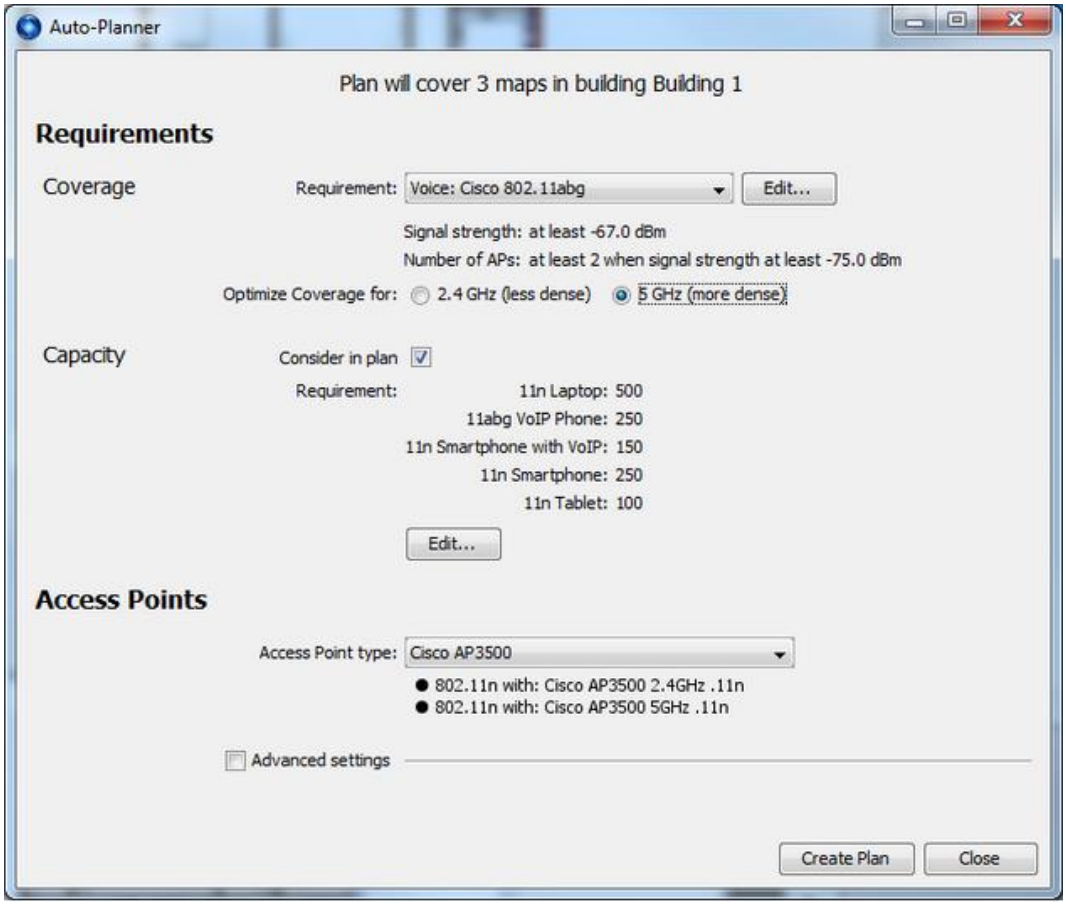
Jotta mittaukset voitiin luotettavasti suorittaa, tarvittiin asianmukaiset laitteet. Lahden ammattikorkeakoulu on aikaisemmin hankkinut tietoliikennetekniikan kursseja varten Ekahau Site Survey -nimisen ohjelman ja kannettavan tietokoneen, johon sai erillisen verkkokortti-adapterin kiinni. Ekahau Site Survey mahdollistaa langattoman verkon kuuluvuuden mittaamisen joko olemassa olevalle WLANille tai täysin uuden suunnittelulle. Ohjelmistoon täytyi ensin

ladata mitattavan rakennuksen pohjapiirrustukset PNG-kuvamuodossa ja määrittää mittakaava, jotta tulokset olisivat luotettavia ja tarkkoja. Mittauksen aikana pohjapiirustukseen merkitään mittaajan sijainti, jotta juuri oikeasta kohdasta saadaan kuuluvuus kartalle. Mittauksien päätyttyä, ohjelma luo pohjapiirustuksen päälle kuuluvuuskartan, josta ilmenee tukiasemat ja mitä verkkoja ohjelma havaitsi. Ekahau myös värittää kuuluvuudet (desibeleissä) vihreästä punaiseen sen mukaan, mitä kuuluvuus oikeasti oli (KUVIO 16).

KUVIO 16. Ekahau Site Survey piirtää graafisesti kuuluvuudet ja tukiasema sijainnit mittauksen jälkeen

Tukiasemien sijainnit Ekahaun kartassa ovat viitteitä antavia, mutta kuuluvuuskarttaa lukemalla tukiasemat löytää melko hyvin. Mittauksien jälkeen kuuluvuuskartasta eroteltiin pois kaikki muut verkot paitsi Lamk student, sillä muuten kartan grafiikka vääristyisi liikaa. Karsinta oli myös hyvä suorittaa, koska

Ekahau tunnistaa kaikki alueella toimivat liityntäpisteet ja käsittelyssä oli ainoastaan Lamk student. Ohjelmassa on myös mahdollista suorittaa Auto-Planner -toiminto, joka tarkoittaa automaattista suunnittelua. Käytännössä tämä tarkoittaa sitä, että Auto-Plannerissä käytettävät alueet (KUVIO 16 sini-valkoinen katkoviiva) määritellään kuuluvuuskarttaan ja tämän jälkeen ohjelma ehdottaa parannukset verkkoon piirtämällä ylimääräisiä tukiasemia. Auto-Planner-tilassa (KUVIO 17) pystyy myös määrittelemään tarkemmin, minkä tyyppisiä tukiasemia halutaan käyttää, lähetystehon vaatimukset sekä mitä kanavia käytetään. Valikoista löytyy myös monia muita kriteerejä ja asetuksia, joita pystyy asettamaan, mutta tässä työssä ei ollut tarve määrittää jokaista asetusta.



KUVIO 17. Auto-Planner -tilan määrityksiä tukiasemille (Ekahau 2012)

Tietohallinnosta tuli myös ohjeistus suorittaa mittaukset Muotoilu- ja Taideinstituutin pääovien ulkopuolella, sillä opiskelijat käyttävät tätä aluetta myös opiskeluun, mikäli sää on sen mukaista. Samalla tietohallinnosta tuli pyyntö, että Kannaksenkadulla samassa rakennuksessa oleva Koulutuskeskus Salpauksen tilat mitattaisiin ja näihin suoritettaisiin myös mahdollisia parannuksia.

4.3 WLAN-mittauksien analysointi

Muotoilu- ja Taideinstituutin tilanne on haastava: ATK-luokkia on sijoitettu paikkoihin, joissa on paksuja betoniseiniä (esimerkkinä väestönsuoja) ja tukiasemia on harvakseltaan. Kuuluvuuskartassa tilanne ei näytä välttämättä huonolta, mutta kapasiteetti on ongelma. Ongelmana on myös ollut vanhemman mallisien tukiasemien (Cisco Aironet 1142-sarjalaiset) kapasiteetin riittämättömyys alueilla, joissa on paljon käyttäjiä. Kun opiskelijoita on liittynyt tukiasemaan monta samanaikaisesti, yhteysnopeudet hidastuvat ja osalla käyttäjistä yhteys jopa katkeaa. Instituutille oli hankittu kolme uudempaa ja ominaisuuksiltaan parempaa saman Cisco Aironetin reititintä luokkiin, joissa käyttöaste on suurempi. Näissä luokissa liikennöinti oli opettajien mukaan parantunut. Varsinaisiin kapasiteetin testauksiin ei resurssit ja aika valitettavasti riittäneet.

Kuuluvuuskarttoja katsomalla voidaan kuitenkin huomata, että suurin osa luokista on kuuluvuudeltaan hyviä: Auto-Planner-ohjelma suositteli lisäämään jokaiseen kerrokseen kaksi tai kolme reititintä lisää. Ulkoalueen kuuluvuus on heikko, ja yksi tukiasema pitäisi sijoittaa sinne, jos halutaan käyttää Lamk student -verkkoa ulkona. Auto-Plannerin tekemää suunnitelmaa ei kuitenkaan pidä täysin noudattaa: lisättäväksi ehdotetut reitittimet voivat sijaita paikoissa, joihin ei ole saatavilla kytkentää sähköverkkoon ja oikeaoppisen uuden WLAN-verkon toteuttamisessa pitäisi käyttää ensin testiympäristöä. Lisäksi tukiasemien eri ominaisuuksien vertailu pitäisi suorittaa ja, että onko välttämättä Ciscon Aironet 1142-sarja paras mahdollinen tämänkokoiseen verkkoon, kun esimerkiksi MASTOnet käyttää Cisco Aironetin 3700-sarjan reitittimiä lisäantennien kanssa. Heikot kuuluvuudet ja reitittimien pitkä väli keskenään aiheuttavat huonot

kuuluvuudet käytävillä (KUVIO 18, KUVIO 19, KUVIO 20), joissa desibeliä merkitsevä väri käy paikoittain keltaisen (noin -50 desibeliä) puolella.

Kuuluvuuskartoituksen lisäksi jokaisesta opetukseen liittyvään luokkaan suoritettiin nopeusmittauksia, joilla pystytään määritelemään datan vastaanotto- ja lähetysnopeudet, joita langattomassa verkossa toimivat laitteet hyödyntää. Nopeusmittauksia suoritettiin jokaiseen opetustilaan useampi ja näistä mittauksista laskettiin keskiarvo vastaanotto- ja lähetysnopeuksille. Parannussuunnitelmaa tehtäessä vastaanotto- ja lähetysnopeuden keskiarvon yhdistäminen ja vertailu kuuluvuuskartan kanssa antaa mahdollisimman hyvän käsityksen langattoman verkon tilanteesta ja mahdollistaa tukiasemien sijoittamisen ongelma-alueille (TAULUKKO 4, TAULUKKO 5, TAULUKKO 6).

TAULUKKO 4. Opiskelijoiden käyttämät tilat kerroksittain vastaanotto- ja lähetysnopeuden keskiarvojen kanssa, sekä tukiaseman tarve sijoittaa opetustilaan

	A-RAKENNUS		Mbps		
		Ping (ms)	Lataus	Lähetys	Tarve tukiasemalle
1.kerros	Porrasaula	15	19,8	18,1	
	Pimeähuone, A-113	16	25,5	35,7	
	Työtila /ETV, A-128	13	21,9	20,3	x
	ETV, A-126	13	53,2	54	
	Apple-TV, A-125	13	53,6	54,2	
	A-123	12	47,8	48,9	
2.kerros	Porrasaula	14	16,8	16,7	
	Käytävä	12	21,3	19,8	
	A-212	12	17,7	13,5	
	A-220	13	17,2	10,4	
	VK-studio, A-201	12	16,2	16,1	x
	Ari Mirja, teorialuokka	13	12,1	11,5	x
3.Kerros	Apple-TV, A-320	13	55,9	55,9	
	GR, A-317	13	41,5	42,9	
	PAMU, A-316	13	16,2	18,4	x
	PAMU, A-305	13	18,8	18,8	
	GR, A-326	14	14,8	13,4	x

TAULUKKO 5. Opiskelijoiden käyttämät tilat kerroksittain vastaanotto- ja lähetysnopeuden keskiarvojen kanssa, sekä tukiaseman tarve sijoittaa opetustilaan

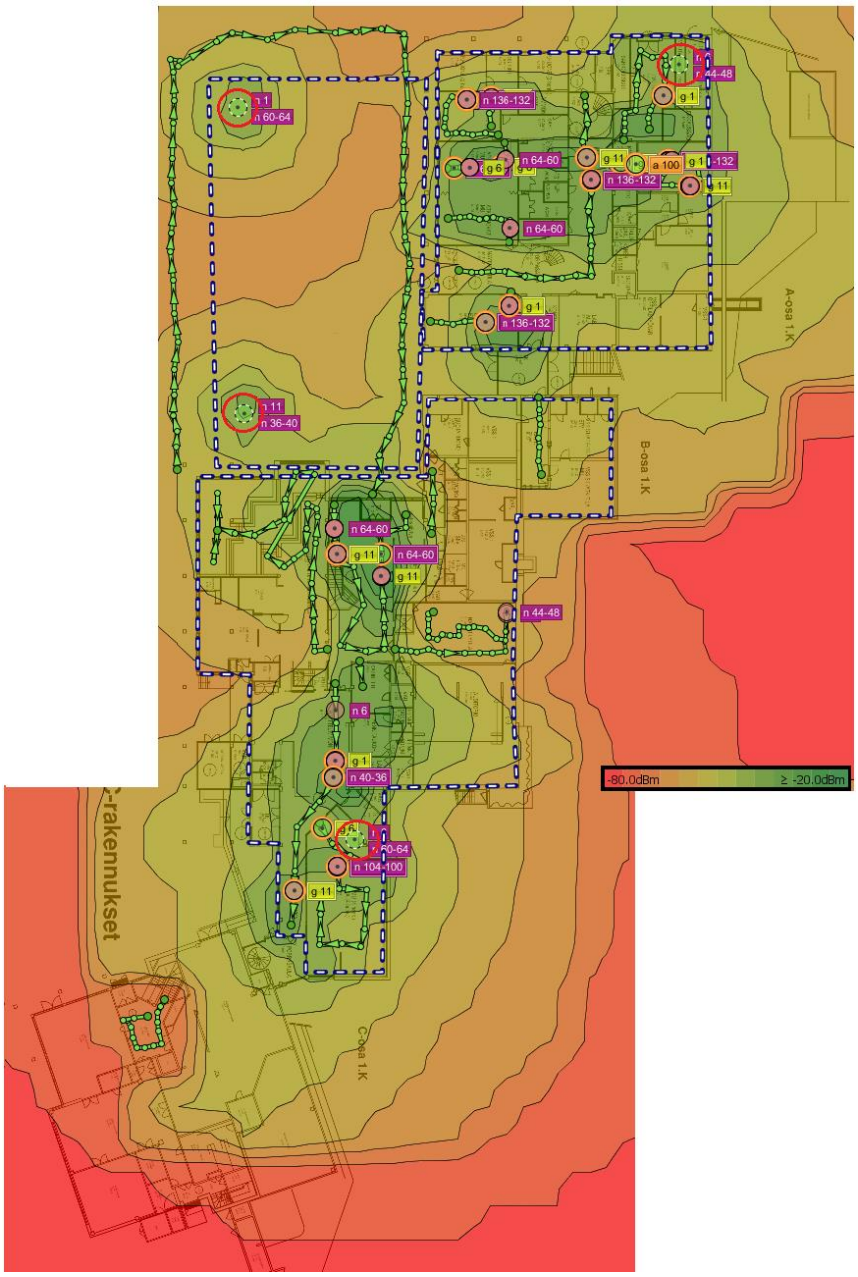
	B-RAKENNUS		Mbps	
		Ping (ms)	Lataus	Lähetys	Tarve tukiasemalle
1.kerros	B-aula	14	19,6	19,6	
	B aulan auditorio	5	9,6	8,3	2.kerroksen auditorio kattaa
	RUOKALA	14	18,8	19,6	
	Näyttely/monitoimitila, B-114	14	44,5	53,1	
	TEMU, B-118	9	53,7	51,6	
2.kerros	Näyttelytila/aula, B-203	11	35,1	52,1	
	Auditorio	9	20,3	20,5	
	Neuvottelutila, B-216	16	8,1	2,2	x
	Kritiikki-näyttelytila, B-213a	11	49,7	48,8	
	Esinemuotoilu, B-241	12	21,2	21,3	
3.kerros	Näyttelytila/aula, B-303	15	14,2	17,8	
	Arkkitehtuuri	11	21,4	21,7	
	SIKA ATK, B-320	13	22,1	21,6	
	MU-VA, B-326	9	19,7	18,9	
	MU-VA, B-333	12	59,4	54,2	
	MU-VA, B-331	9	45,7	43,2	x
	MU-VA, B-332	13	54,1	56,8	
	MU-VA, B-328	14	20,6	19,8	
	Ompelimo, B-315	14	17,1	20	
	SIKA, B-317	12	19,4	19,3	
	SIKA, B-316	13	22,4	20,5	x
	SIKA, B-314	13	19,9	19,8	
	PAMU, B-307	12	19,9	19,8	
	PAMU, B-306	12	4,8	7,7	x
	TEMU, B-304	15	4,2	0,3	B-306 kattaa
	TEMU, B-305	14	8,9	11,6	x

TAULUKKO 6. Opiskelijoiden käyttämät tilat kerroksittain vastaanotto- ja lähetysnopeuden keskiarvojen kanssa, sekä tukiaseman tarve sijoittaa opetustilaan

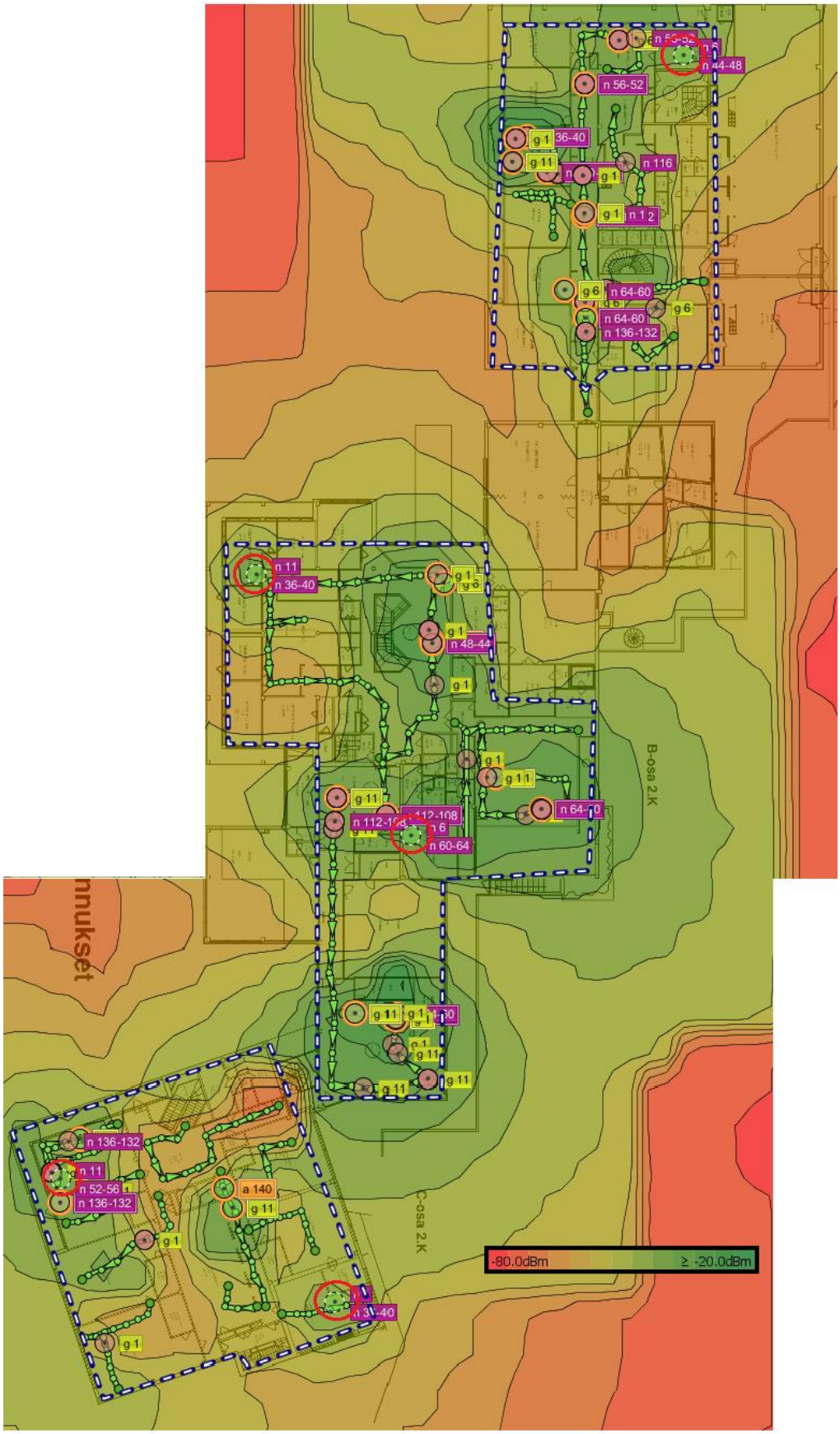
	C-RAKENNUS		Mbps	
		Ping (ms)	Lataus	Lähetys	Tarve tukiasemalle
2.kerros	KIPSI, C-216	10	3	0,6	C-215 kattaa
	Mallityötila, C-215	14	7	15	x
	AMK 1.luokka, C-204	9	11,7	4,2	x
	Konekaiverrus	13	20,8	20,2	
	C-202	12	20,1	18,5	x

Tukiasemien sijoittamisessa on otettu huomioon luokkien käyttöaste. Nopeusmittauksien tuloksia on vertailtu kuuluvuuskarttaan myös siten, että jo olemassa olevat tukiasemat otettu huomioon. Lisäksi suunnitelmassa on otettu huomioon nykyisten tukiasemien sijainnit ja kuuluvuudet. Vaikka opetustilalle nopeusmittauksen tulos on huono, pystytään kuuluvuus ja nopeus korjaamaan sijoittamalla tukiasema viereiseen opetustilaan, joka on saanut yhtä huonot nopeusmittauksen tulokset.

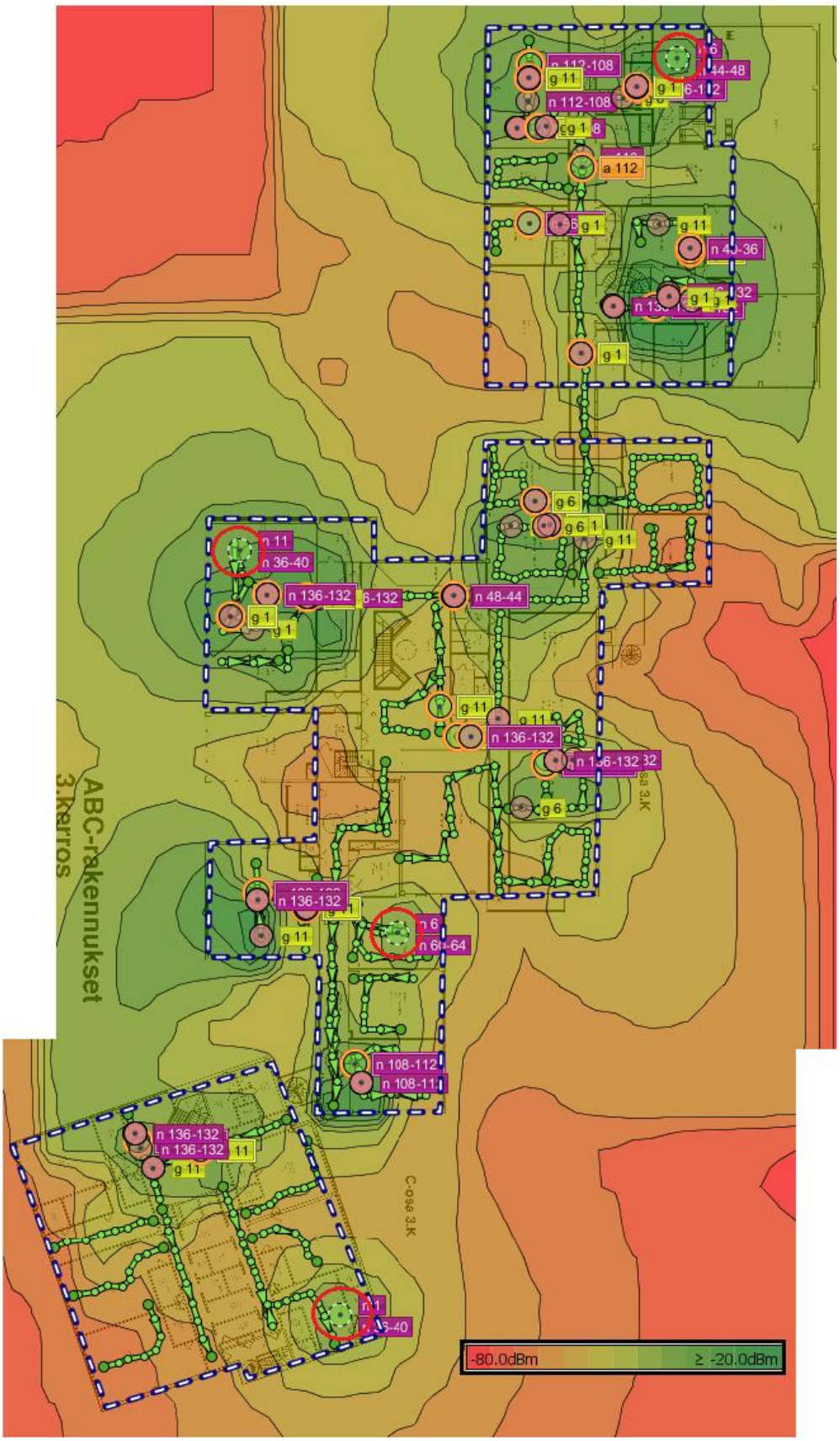
Mikäli Lamk student -verkkoa haluttaisiin kunnolla parantaa, täytyisi ensin miettiä Ekahau-ohjelman päivittämistä uudempaan versioon. LAMKin käytössä oleva ohjelmisto on vanha, ja uudemmassa ohjelmistossa pystyy määrittelemään tarkemmin esimerkiksi seinien materiaalit ja muita mittauksille tärkeitä ominaisuuksia. Seuraavaksi tulisi suorittaa testiympäristön rakentamisen, kapasiteettimittaukset testiympäristön kautta pitkäjänteisellä testaamisella ja sitten vasta ryhtyä suunnitelemaan näiden tulosten pohjalta verkon parantamista suuremmassa mittakaavassa. Muotoilu- ja Taideinstituutin langattoman verkon tilanne ei ole niin huono, kuin annettiin ymmärtää, mutta parannussuunnitelman pohjalta tehdyt muutokset riittävät Lamk student -verkon saamisen sille tasolle, että toiminta verkossa parantuu.



KUVIO 18. Muotoilu- ja Taideinstituutin ensimmäisen kerroksen kuuluvuuskartta. Karttaan on ympyröity punaisella Auto-Plannerin mukaiset lisätukiasemat



KUVIO 19. Muotoilu- ja Taideinstituutin toisen kerroksen kuuluvuuskartta. Karttaan on ympyröity punaisella Auto-Plannerin mukaiset lisä-tukiasemat



KUVIO 20. Muotoilu- ja Taideinstituutin kolmannen kerroksen kuuluvuuskartta. Karttaan on ympyröity punaisella Auto-Plannerin mukaiset lisä-tukiasemat

5 YHTEENVETO

Lahden ammattikorkeakoulussa halutaan parantaa opiskelijoiden oppimiskäytäntöjä ja varsinkin etätyöskentelyä. Syyslukukaudella aloitettava BYOD tuo LAMK:n opiskelijoille mahdollisuuden käyttää omia laitteitaan turvallisesti suljetussa verkossa koulutehtäviä varten. Lahden alueella toimii jo MASTOnet langaton lähiverkko, joka on ilmainen eikä vaadi yksilöllistä kirjautumista verkkoon. LAMK:ssa käytettävä Lamk student -verkko on kuitenkin suljettu ja opiskelijoille annetaan SSID-tunnus kirjautumista varten. Lisäksi selainsivulle aukeavaan kirjautumiskenttään täytyy syöttää omat AD-tunnuksensa, jotta verkossa liikennöinti on mahdollista.

Lamk student -verkon kanssa on ollut haasteita, ja se onkin suhteellisen alkutekijöissään. Verkon kattavuus on tyydyttävällä tasolla ja nyt Tietohallinnon pyynnöstä verkon kapasiteetti haluttiin kartoittaa Kannaksenkadun Muotoilu- ja Taideinstituutin sekä Ståhlberginkadun Tekniikan laitoksen tilojen puolesta. Tässä opinnäytetyössä on käsitelty WLAN-tekniikkaa teoriassa ja lukija perehdytetään langattoman lähiverkon yleisimpiin ominaisuuksiin, sovellutuksiin ja käyttöön. Toisena osana tässä opinnäytetyössä on keskitytty Muotoilu- ja Taideinstituutin langattoman verkon kuntoon ja sen parannusehdotukseen. Käytännön osuudessa on myös esitelty mittauksia varten käytettyä tekniikkaa, Ekahau Site Survey, jolla on mahdollista mitata, suunnitella ja analysoida verkkoa juuri sellaisena kuin se on. Lisäksi parannussuunnitelmassa on hyödynnetty datan vastaanotto- ja lähetysnopeuksien vertailua kuuluvuuskarttaan, joita vertailemalla on saatu kattava kuva langattoman verkon nykyisestä tilasta ja, mihin opetustiloihin täytyisi lisätä tukiasemia kapasiteetin ja kuuluvuuden parantamiseksi. Tässä opinnäytetyössä ei kuitenkaan ole toteutettu ajanpuutteen takia verkkosuunnittelua siten, miten se pitäisi tehdä: Ensin suoritetaan verkon kuuluvuuskartoitus, jonka jälkeen tehdään pienimuotoinen testiympäristö verkon testausta varten. Testiympäristön täytyy myös vastata analysoitavaa verkkoa ja kapasiteettitestausta täytyy tehdä tarpeeksi pitkään. Näiden vaiheiden jälkeen suoritettaisiin suunnitelma, jossa käsiteltäisiin verkkoon tarvittavia muutoksia.

Ekahau -ohjelmistossa oleva Auto-Planner-ohjelma toi mahdollisuuden suorittaa graafisesti näytettäviin kuuluvuuskarttoihin optimaaliset parannusehdotukset,

ainakin ohjelmiston mielestä. Ekahau-ohjelmassa ei pystytä määrittelemään, miten sähköverkosto rakennukseen on rakennettu ja tästä syystä ohjelman ehdottamat tukiasemat voivat olla mitä merkillisimmissä paikoissa, tai sähköverkon ja kiinteään lähiverkkoon liittämisen kannalta huonoissa paikoissa. Muotoilu- ja Taideinstituutin rakennukset ovat myös yleisesti ottaen haasteellisia WLAN-verkon suorittamiselle: rakennuksia on kolme eri siipeä ja jokainen on kolmessa eri kerroksessa (LIITE 1, LIITE 2, LIITE 3). Tämä tarkoittaa sitä, että tukiasemia täytyy olla monta, tietenkin kantavuudesta riippuen, mutta lähtökohtaisesti luokkien seinät syövät kuuluvuutta. Myöskään kerrosten väliset kuuluvuudet eivät ole laadukkaita ja etenkin alimmassa kerroksessa sijaitsevien ATK-luokkien WLAN-kuuluvuus on erittäin heikko. Pidemmälle tulevaisuutta varten ajatellen täytyisi suorittaa pidemmällä aikavälillä verkon testausta ja tehdä jopa radikaaleja ratkaisuja verkon infrastruktuuriin.

Yrityksien kannalta WLAN-verkko ei ole välttämätön, mutta yleisen käytännöllisyyden perusteella langaton verkko tuo hyötynsä suuresti esille. Jo pelkästään vierailevien asiakkaiden näkökulmasta langaton verkko tuo positiivista ja toiminnallisuuden kuvaa yrityksestä, johon asiakas on tullut vierailemaan. Langaton verkko on myös tärkeä osa yrityksiä, joilla ei ole mahdollisuutta luoda normaalia langallista yhteyttä esimerkiksi viereiseen yrityksen omistamaan toimipisteeseen. Mahdollisuuksia on monia, ja hyötyjä on lähtökohtaisesti enemmän kuin haittoja: tietoturva on suurin uhka, joka yrityksellä voi olla, mutta ammattitasoisella järjestelmänhallinnalla nämä uhat voidaan eliminoida.

LÄHTEET

Axis. 2015. Local area network and Ethernet [viitattu 12.3.2015]. Saatavissa: http://www.axis.com/products/video/about_networkvideo/ip_networks.htm

Cisco. 2015. Cisco Wireless LAN Security Overview [viitattu 20.3.2015]. Saatavissa: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-point/prod_brochure09186a00801f7d0b.html

Cisco Press. 2015. Internetworking Basics [viitattu 19.3.2015]. Saatavissa: http://www.cisco.com/cpress/cc/td/cpress/fund/ith/ith01gb.htm

Tietojenkäsittelytieteen laitos. 2015. Otteita rikoslaista [viitattu 20.3.2015]. Saatavissa: https://www.cs.helsinki.fi/compfac/rikoslaki.html

EE Herald. 2015. Data Communication Standards and Protocols [viitattu 12.3.2015]. Saatavissa: http://www.eeherald.com/section/design-guide/ieee802_3.html

Ekahau. 2012. Unlock the power of your wireless network! [viitattu 23.3.2015]. Saatavissa: http://www.ekahau.com/real-time-location-system/blog/category/wi-fi-planning/page/2/?excerpt=more

Extremetech. 2014. How to boost your WiFi speed by choosing the right channel [17.3.2015]. Saatavissa: http://www.extremetech.com/computing/179344-how-to-boost-your-wifi-speed-by-choosing-the-right-channel

For Dummies. 2015. Cisco Networking: Data Framing [viitattu 16.3.2015]. Saatavissa: http://www.dummies.com/how-to/content/cisco-networking-data-framing.html

Juutilainen. 2007. Lappeenranta University of Technology. Siirtyvä tietoliikenne [viitattu 16.3.2015]. Saatavissa: http://www2.it.lut.fi/kurssit/06-07/Ti5312600/luentokalvot/luento03.pdf

Lowe, D. 2013. Networking for Dummies. 10. painos. Hoboken, New Jersey: John Wiley & Sons, Inc.

PlurarSight. 2011. Wireless Security Considerations: Common Security Threats to Wireless Networks [viitattu 20.3.2015]. Saatavissa: http://blog.pluralsight.com/wireless-lan-security-threats

Radio-Electronics. 2015. Wi-Fi / WLAN Channels, Frequencies, Bands & Bandwidths [viittattu 17.3.2015]. Saatavissa: http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php

Rousku. 2013. Miten suojautua kohdistetuilta hyökkäyksiltä? [viitattu 21.3.2015]. Saatavissa: http://www.tivi.fi/blogit/2013-11-07/Miten-suojautua-kohdistetuilta-hy%C3%B6kk%C3%A4yksilt%C3%A4-3205431.html

Suomen Standardisoimisliitto. SFS-Käsikirja 19. 2001. Suureet ja yksiköt. SI-mittayksikköjärjestelmä. Helsinki [viitattu 10.3.2015]. Saatavissa: http://web.archive.org/web/20120831234747/http://www.sfs.fi/files/70/si-opas.pdf

Signal Partners. 2015. Verkkokartoitukset ja verkon suunnittelu [viitattu 22.3.2015]. Saatavissa: http://www.signalpartners.fi/verkkokartoitukset-ja-verkon-suunnittelu/

Techopedia. 2015. Wireless Local Area Network [viitattu 14.3.2015]. Saatavissa: http://www.techopedia.com/definition/5107/wireless-local-area-network-wlan

TP-Link. 2015. The Difference between WPA-Personal and WPA-Enterprise [viitattu 21.3.2015]. Saatavissa: http://www.tp-link.com/en/article/?faqid=500

Vähä-Touru, T. 2007. Langattoman lähiverkon toteutus. Tampere: Tampereen ammattikorkeakoulu [viitattu 22.3.2015]. AMK-opinnäytetyö. Saatavissa: http://urn.fi/URN:NBN:fi:amk-201003064925

Verkkokauppa.com. 2015. Helikopterit, 3-kanavaiset [viitattu 13.3.2015]. Saatavissa: http://www.verkkokauppa.com/fi/product/13725/dmjqv/RedBird-2-4-GHz-kauko-ohjattava-3-kanavainen-helikopteri-vid

Webopedia. 2015a. CSMA/CD [viitattu 17.3.2015]. Saatavissa: http://www.webopedia.com/TERM/C/CSMA_CD.html

Webopedia. 2015b. Wireless Networking Standards [viitattu 17.3.2015]. Saatavissa: http://www.webopedia.com/quick_ref/WLANStandards.asp

Wikipedia. 2015a. Amplitude modulation [viitattu 16.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Amplitude_modulation

Wikipedia. 2015b. Cambridge Ring [viitattu 10.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Cambridge_Ring_(computer_network)

Wikipedia. 2015c. Ethernet [viitattu 10.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Ethernet

Wikipedia. 2015d. PARC [viitattu 10.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/PARC_(company)

Wikipedia. 2015e. Phase [viitattu 16.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Phase_(waves)

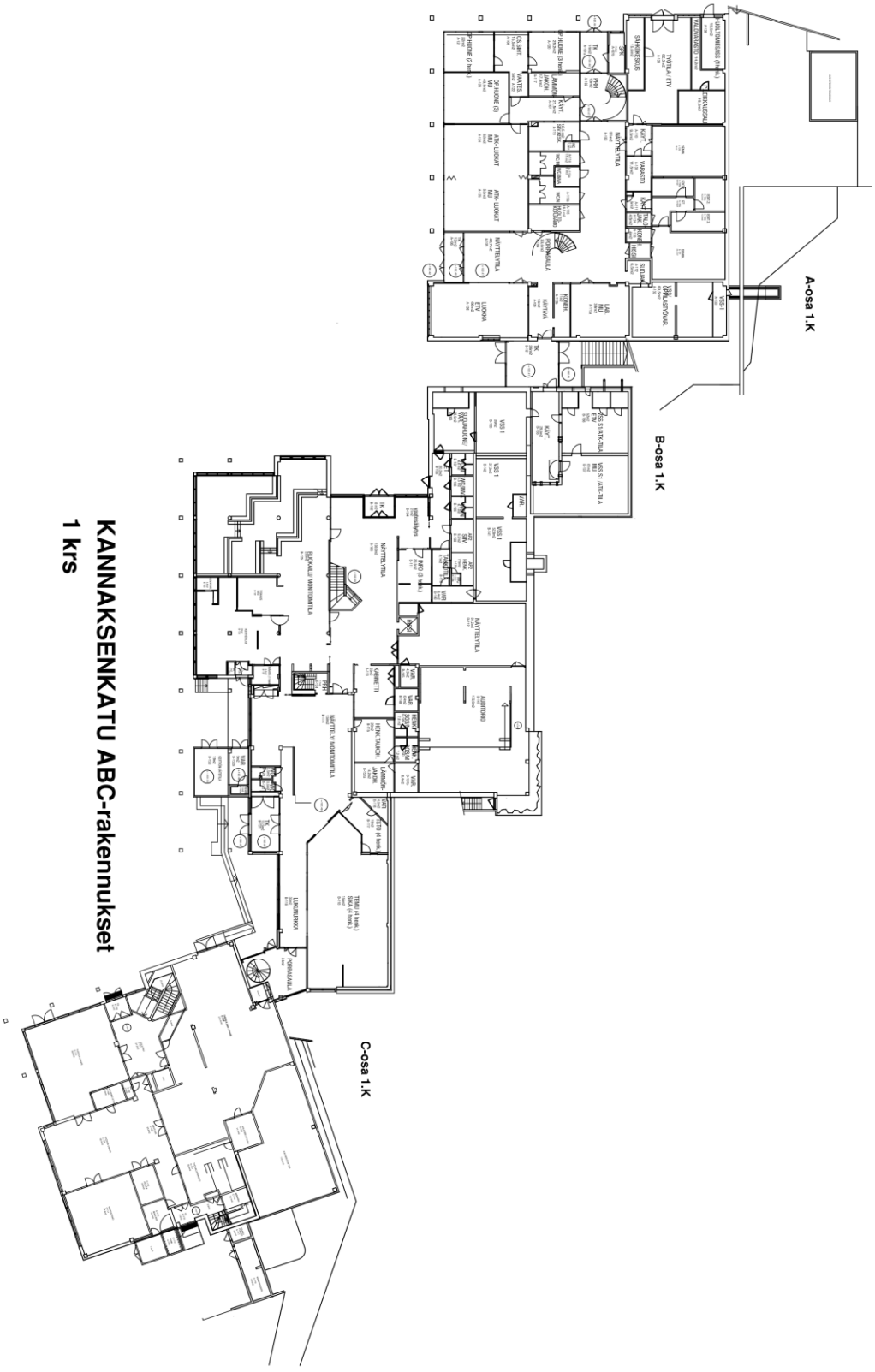
Wikipedia. 2015f. SSID [viitattu 14.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Service_set_(802.11_network)

Wikipedia 2015g. Wi-Fi Protected Access [viitattu 21.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

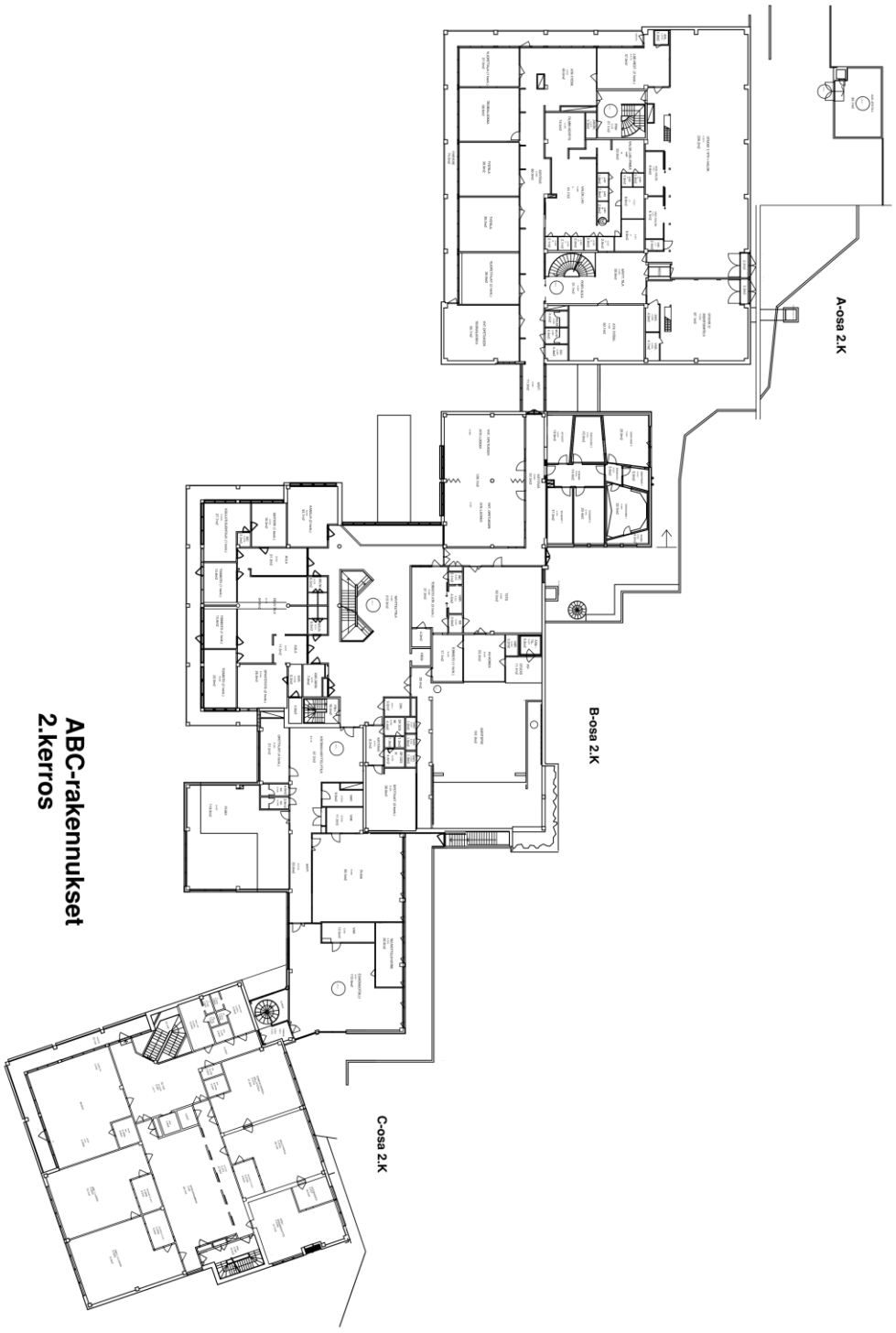
Wikipedia. 2015h. WLAN [viitattu 13.3.2015]. Saatavissa: http://en.wikipedia.org/wiki/Wireless_LAN

LIITTEET

LIITE 1. Muotoilu- ja Taideinstuutin ensimmäisen kerroksen pohjapiirrustus.



LIITE 2. Muotoilu- ja Taideinstuutin toisen kerroksen pohjapiirrustus.



LIITE 3. Muotoilu- ja Taideinstuutin kolmannen kerroksen pohjapiirrustus.